Fundamentals of Internet Policy

Selected Topics

Table of Contents

FOREWORD

Dear Colleague:

Today, more than ever before, digital policy choices can have an extraordinarily large impact on U.S. economic interests. The modern digital economy represents a significant portion of U.S. commerce, and it is a cornerstone of crossborder trade in goods and services. The Internet accounts for at least 6% of U.S. GDP and 3 million American jobs. Notably, the U.S. Internet sector leads the world, generating an overwhelming $159 billion digital trade surplus for the U.S. economy. Businesses small and large, and industries both traditional and new rely upon the Internet to export goods and services to foreign markets worldwide.

The growing impact of the Internet on global productivity and commerce has coincided with the rise of policies that hinder its potential and impede digital trade. The success of the Internet has been directly attributable to wise U.S. policies: globalizing that success is contingent on sound public policy abroad. Just as smart policy can grow export markets and promote job creation, unsound policies can reverse these gains.

Unfortunately the challenges are many. In some jurisdictions, lawful Internet platforms and online content are blocked or filtered, often without transparent judicial processes. Some governments also implement policies that mandate the localization of servers and data within their borders.

Other challenges include "shoot the messenger" rules, where lawful online services are subjected to civil or criminal liability for misconduct perpetrated by Internet users. While the United States and some other countries have provided legal protections to online services that respond promptly to complaints, other jurisdictions penalize intermediaries for the misconduct of others.

Digital economy exporters are also confronted with imbalanced copyright laws which do not accommodate new innovations like machine learning, or which seek to tax the act of quotation. U.S. exports are also at risk from restrictive policies relating to foreign investment, often intended to protect domestic incumbents, and customs policies drafted in the pre-Internet era.

This collection of readings can serve as a reference to policymakers who must confront these and other new challenges, so as to enable the digital economy and realize its full potential to create jobs and opportunity.

Ed Black
CEO
Computer & Communications
Industry Association

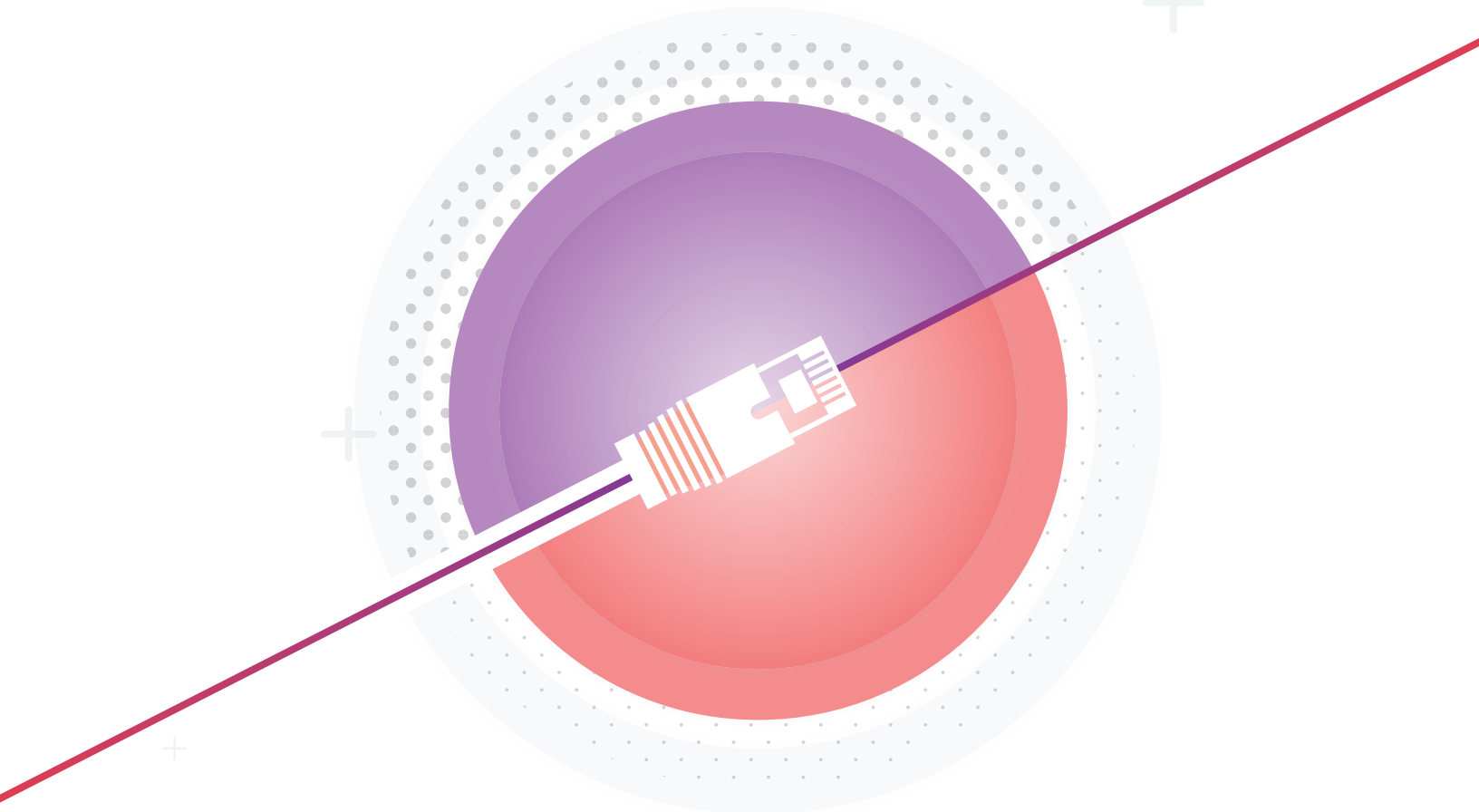
Michael Beckerman
CEO
Internet Association

INNOVATION ECONOMY

Introduction to the Internet Economy

Refreshing Our Understanding of the Internet Economy

By Christopher Hooton, Ph.D.



Dear internet users,

How big is the internet? It seems like a basic question, but there is no simple answer because the internet is not a single monolith. Unlike the auto industry, which can be measured in terms of cars produced or manufacturing plants built, the internet's massive economic contribution spans nearly every industry, and it is even creating entirely new industries. In the U.S. economy alone, it comprised approximately 6% of GDP in 2014 and has continued to grow rapidly, driving innovation at a faster rate than we have ever seen in human history.

More than 3.2 billion people use the internet, yet, if you ask most of us to tell you what "the internet" is, we may lack the right words to describe it. We understand how to use internet-enabled tools for everything from managing personal finances, to diagnosing illnesses, to ordering food from our favorite restaurants. Yet, we still struggle to accurately quantify the full impact of ubiquitous internet technology on our lives. For most, a full conceptual appreciation of the internet is neither necessary nor important; but, for policymakers, regulators, and other active stakeholders, we need to begin moving past outdated ideas and perceptions about the internet as a monolithic economic entity and recognize its nuances and complexities.

Too often policies and regulations for the internet are designed and implemented without any real appreciation for their short- or long-term impact. Often, this arises from a misunderstanding of the sector as a whole or from a misunderstanding of the particular platform or service model being targeted. The internet is not measured officially through industrial classification codes and the unofficial methods that have been developed by researchers are almost certainly too conservative. The classification codes that do exist poorly capture the full range of internet goods and services.

The negative consequences of these outdated methods for classification and assessment are not just academic. Businesses that didn't exist just two or three years ago are being treated the same as industries created over a century ago. Regulations designed in the Great Depression are being applied to inventions that – even ten years ago – were outside the imaginations of even the greatest science fiction writers.

The lag between policy design and the innovation of the internet and its businesses is understandable given the sheer speed with which the internet has moved, but it is time to catch up. Designing internet regulations without properly understanding the sector can seriously undermine the success of its businesses and users for years to come. The Internet Association presents this white paper as a first step in refreshing the dialogue between the industry, policymakers, and other stakeholders to help avert poorly-informed policy decisions. It offers the first attempt to compile economic contribution estimates for the internet, calculates the first estimate of the economic contribution of mobile internet and app services to the economy, and lays out a better approach to conceptualizing the internet within our economic taxonomy. The goal is not to solve these issues in their entirety, but rather start the conversation and reinvigorate it with nuance, analysis, and consideration.

Sincerely,

Christopher Hooton, Ph.D.
Chief Economist, The Internet Association

Contents

Section A /

Introduction

What was your first memory of the internet? A howling dial-up? Chat room sessions with your friends? Sending an email on your phone? Setting up a social media account? No matter your age or familiarity level, chances are the image is outdated.

The internet has long since evolved into a rich and diverse ecosystem of new platforms, businesses, and resources that have fundamentally changed the way in which markets function. In many ways, it has been the great economic equalizer, enabling low-cost entry and exit to firms, instant information to actors, transformation of consumer expectations, and the creation of a geographically neutral market where actors from different ends of the globe can connect and effectively interact regardless of borders. It is opening up new competition and pushing forward the frontier of production as it disrupts entrenched industries, sometimes provoking well-intentioned, but ill-advised reactions. It is fast – essentially instantaneous. It is open. And its evolution has and continues to outpace our attempts to grapple with it in research and policy.

The importance of the internet's role in the global economy and national markets is under-researched and underappreciated. However, beyond matters of attention and scale, the manner in which we conceptualize and approach the internet must also change. It is no longer sufficient from an economic and policy standpoint to lump together the whole of the "Internet" into one amorphous thing. It requires more nuance in how we understand its economic contributions and more depth in the analysis that tries to quantify and make sense of it.

To that end this white paper calls for a modernized appreciation of what the internet does for our economy and presents a summation of recent literature to illustrate how and why such an exercise is needed. The paper begins in Section B by recapping studies examining the economic contributions of the internet, which as of 2014 stood at approximately 6% of GDP in the United States with every indication of continued growth (Siwek, 2015), and trying to more explicitly connect the internet to appreciable comparators. The section serves as a reminder of the economic importance of the internet and its activities and as a thought exercise for better ways to consider it going forward. Next, in Section C the paper extends these themes to the unofficial subsector of mobile internet and apps with the goal of demonstrating the logic and importance of improved economic classification. The paper applies the results and model of Christensen et al. (2015), which modeled the per unit GDP per capita contributions of smartphones and tablets (as a comparable for the examination of potential future impacts from Augmented Reality and Virtual Reality units) to figures found on usage from Pew and the National Research Council. From this it calculates a 3.11% GDP contribution from mobile internet and app services in the United States for 2015. The finding reinforces previous estimates of total GDP contributions from the internet sector as a whole and demonstrates the overdue importance of examining the internet in more detail. Building off Sections B and C, Section D proposes two alternative approaches to future economic conceptualizations of the internet through the use of industrial classification systems as a commencement to the dialogue in how to improve our conceptualization of the sector. Finally, Section E concludes.

"What was your first memory of the internet? No matter your age or familiarity level, chances are the image is outdated.

The goal of the paper is not to resolve all issues related to the discussion of the internet in the economy, but simply to reignite the conversation. The issues raised here require more than a 15-page white paper to fully examine and the potential range of outcomes from them for businesses, consumers, households, and other stakeholders demand a more constructive dialogue involving all parties. This is an attempt to start that dialogue.

Section B /

What We Know About the Internet

The unfortunate truth is that much of what we know about the internet is several years old, meaning that how we describe it is often incomplete and, given the dramatic rapidity of its growth and development, generally overly conservative. Yes, the internet is big. Yes, the services and products offered by it are diverse and abundant. But without a new more modern approach to our study and consideration of the sector, we will continue to discuss the past state of the sector while it speeds away through innovation and maturation.

The figure of focus over the past decade has been Gross Domestic Product (GDP). Estimates show a significant and consistent contribution across methodologies that has grown rapidly over the past decade. In 2007, the sector was estimated to have contributed 2.94% of the U.S. GDP (Siwek, 2015). In 2009, the estimate was 3.8% of US GDP and in 2010 it was 4.7% (du Rausas et al., 2011; Dean et al., 2012). Using 2011 data, the Organization for Economic Cooperation and Development (OECD) estimated internet-related activities comprised between 3.2% (using conservative estimates) and up to 13.2% of US business sector value added (a component of GDP) (OECD, 2013). They also estimated a 7.1% GDP dynamic contribution to the US economy in 2011 from the internet based on an adapted methodological approach from Koutroumpis (2009). The figure of focus over the past decade has been Gross Domestic Product (GDP). Estimates show a significant and consistent contribution across methodologies that has grown rapidly over the past decade. In 2007, the sector was estimated to have contributed 2.94% of the U.S. GDP (Siwek, 2015). In 2009, the estimate was 3.8% of US GDP and in 2010 it was 4.7% (du Rausas et al., 2011; Dean et al., 2012). Using 2011 data, the Organization for Economic Cooperation and Development (OECD) estimated internet-related activities comprised between 3.2% (using conservative estimates) and up to 13.2% of US business sector value added (a component of GDP) (OECD, 2013). They also estimated a 7.1% GDP dynamic contribution to the US economy in 2011 from the internet based on an adapted methodological approach from Koutroumpis (2009).

Globally, the internet contribution to GDP is similarly high in many developed countries and in pooled estimates. One such calculation put the figure at approximately 3.4% among 13 of the world's largest countries/economies in 2009 (du Rausas et al., 2011). More recently, a global study estimated the GDP contribution at approximately 4.1% of GDP among the G-20 economies in 2010 (Dean et al, 2012).

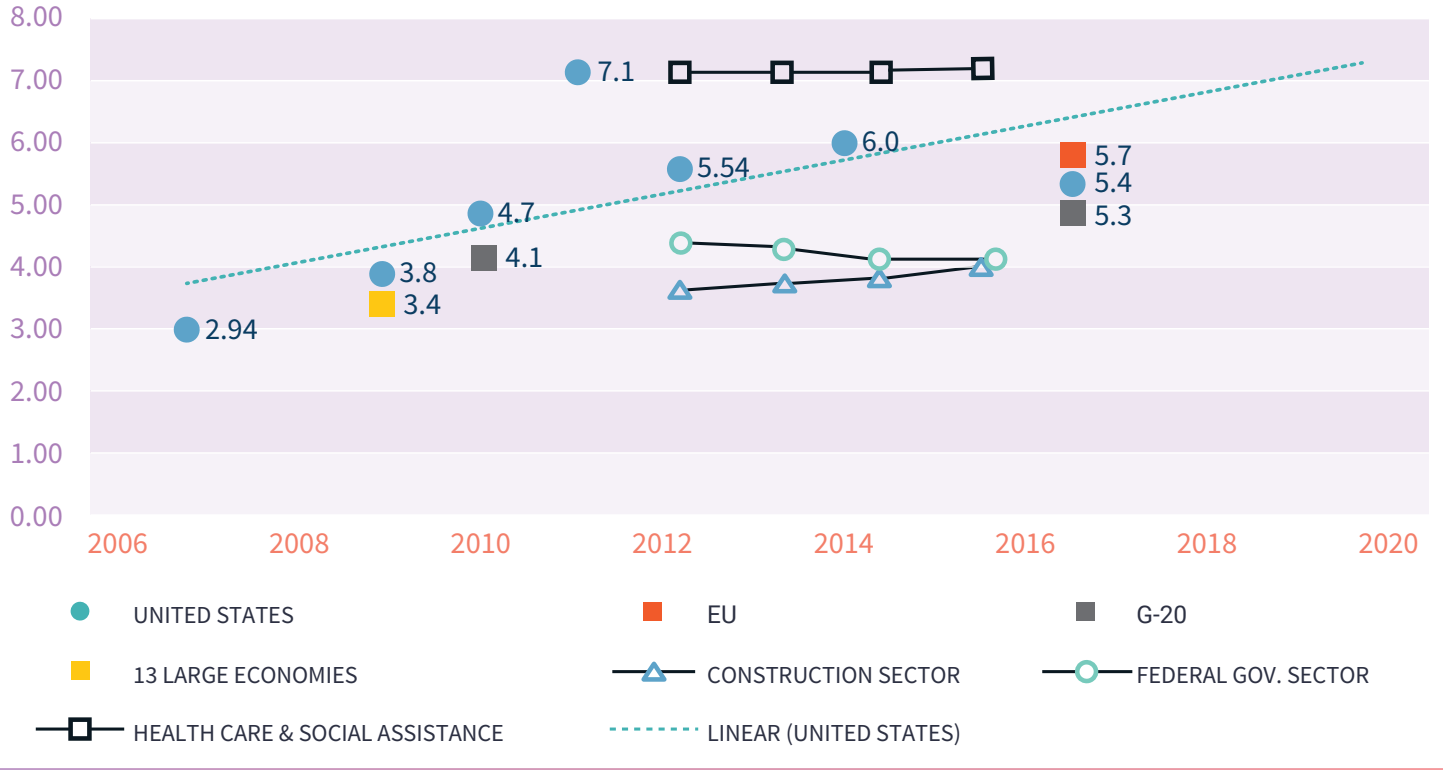
Jumping forward to today's impact, two forecasts from several years ago predicted a rise in the sector's contribution by 2016 to 5.3% and 5.7% of GDP for the G-20 economies and the EU respectively (Dean et al., 2012). And most recently, an analysis conducted in 2015 using data for 2012 found that the internet comprised approximately 6% of GDP (in 2012) in the United States (Siwek, 2015). Table 1 shows these estimates and the forecasted upward (U.S.) trajectory.

> *"Estimates show a significant and consistent contribution [to GDP] across methodologies that has grown rapidly.*

There are several things to note from these studies and estimates. First, the figures are reassuringly similar in size across different researchers and methodologies, which should help to quiet any lingering skepticism on their accuracy. Second, the estimates all either use data that are several years old or are forecasts made from five or more years ago, which highlights the need for improved and more frequent data collection and research. Third, none of the studies provide broad discussion into the full range of components that make up the internet economy[1]. And fourth, across

1 It should be noted that this due to the nature of these studies, which focused on establishing some baseline measurements and, more importantly, methodologies for assessing an analytically tricky sector. Illustrative examples are generally given, but detailed examinations were beyond their scopes.

Table 1 / Internet sector GDP contribution estimates by year with comparators



Source: Author's elaboration; estimates from references cited above in Section C.

the board, these studies cite the lack of and difficulty in identifying appropriate data and classifications to facilitate measurements. The paper focuses on these last two areas, which deal more directly with the conceptualization and the contributions of the internet economy.

Take for example the definition provided by OECD – it defines the Internet economy as, "the full range of our economic, social, and cultural activities supported by the Internetand related information and communications technologies" (OECD, 2008). However, rather than delving into the specific activities, their 2013 study estimating the sector's economic contribution focuses on recapping related literature sets, such as the Information Communication Technology (ICT) infrastructure academic literature, with only limited examination of sectors and subsectors. Furthermore, they focus on providing guidance on methodological approaches highlighting three broad strategies for three different aspects of the internet economy: 1) Direct Impact measurements (through value added); 2) Dynamic Impact measurements (through GDP growth); and, 3) Indirect Impact measurements (through consumer surplus and welfare gains). This is at least likely due, apart from the general usefulness of a more robust review of methodologies, to their admission that the internet economy is an extensive and hard-to-capture sector compared to, for example, a physical infrastructure network which is perhaps more tangible.

This is indeed a common issue among researchers, policymakers, and other stakeholders and the paper argues that it is largely due to the natural tendency to consider the internet sector in the same manner as any other sector. Put differently, there is a tendency to try to simply add the 'internet' into the typology systems of sectors and industries that already exist, such as the North American Industrial Classification System (NAICS). This is an issue for two reasons. First, these systems have yet to fully develop a range of classification codes that is sufficient for the complete spectrum of activities carried out by internet companies. Second, even if a more robust set of codes existed, current classification

systems cannot accommodate the fact that the internet sector offers both a unique subset of new products and services and a new tool for operational improvement that can be applied universally across all other sectors. The internet economy is comprised of both unique industries (e.g. apps exclusively available through the internet) and traditional industrial activities conducted through new tools and platforms from the internet (e.g. a carmaker selling vehicles online as well as through physical dealerships).

Simply placing the internet sector, as it has been measured through the reports cited above, within the current NAICS taxonomy (or other formalized system) produces a deceptively intuitive fit (see Appendix A to see where the internet 'sector' compares to others). Researchers can quickly provide comparators that seem appropriately matched: the internet sector contributes approximately 6% of the US GDP; it is a top-20 industry within the United States economy (in 2015); it is larger than powerhouse sectors such as Construction (3.6% in 2012), Transportation and Warehousing (2.9% in 2012), and others. All of these are true, but as several other researchers who have analyzed the internet economy have argued, the estimates are likely conservative and the comparators are not entirely appropriate.

Perhaps a more useful approach hinted at by du Rausas et al. (2011) is to consider the internet economy as a unique market (i.e. the same way we would a sovereign nation). They estimated that in 2009 the internet would have been one of the 10 largest national economies in the world, larger than Canada, Spain, and many other large developed economies, implying a global GDP contribution of over 2.1%. And while not entirely applicable, the approach does fit many of the economic activities in the internet. Recent years have seen the development and stabilization of new currencies (bitcoin and other cryptocurrencies), the development and sale of new territory (domains and sites), new production and distribution infrastructure systems (apps and network platforms), new communities and culture (social networks), and the collection and utilization of new forms of resources and commodities that can be mined and processed into economically useful items (data, APIs, and more).

> *"The types of goods and services developed via and available through the internet should, at a minimum, be given more attention than they currently receive.*

This is not to suggest that the internet should be considered a country, but it does illustrate that the types of goods and services developed via and available through the internet should, at a minimum, be given more attention than they currently receive and, as the paper argues, considered a unique class with a more sophisticated approach of incorporation.

Section C /

Considering the Internet in a New Set of Lights

Extending the thought experiment to some actual data emphasizes the point. The internet and its subsectors/industries/activities (whichever of the labels you prefer) cannot simply be lumped together or thrown into the classifications that already exist. This can be seen using the subsector of mobile internet and app services, a classification that does not exist officially but which most closely falls under the NAICS codes 5171 (Wired Telecommunications Carriers) and 517919 (All Other Telecommunications) according to the US Census Bureau's current guidance on NAICS codes. Despite this lack of official classification, the paper estimates that its contribution to the US GDP is approximately 3.11%, putting it at approximately the same size as the Automotive industry, which has historically been estimated at approximately 3.0-3.5% of GDP in the US (Center for Automotive Research, 2015). The implication is clear: internet subsectors are themselves major economic activities that should be tracked.

Leaving the formal coding aside, the paper informally defines mobile internet and app services as internet and application (those that are supported by or

conducted through the internet) usage conducted through mobile devices (i.e. smartphones and tablets). Conceptually, anyone who uses a smartphone or tablet will understand what it means to use mobile internet and apps in their day-to-day life. This could involve reserving a Lyft or Uber vehicle on your phone, shopping on Amazon on your tablet while at the airport, or doing part of your tax return via Intuit while you sip coffee and wait for your friends. The volume and economic value of those activities, however, may be surprising precisely because our current classifications of economic activity are outdated. But when we change our perspective just slightly we can see how mobile internet and apps, along with the support services that make them available to hundreds of millions of mobile internet users in the United States, can be just as valuable to the US economy as the entirety of the auto sector (even when excluding the manufacture of the devices).

> *"The paper estimates that [mobile internet & app services] contribution to the US GDP is approximately 3.11%*

To calculate the value of this GDP contribution the paper draws on the three primary sources. The first is a study conducted by Christensen et al. (2015) from the Analysis Group entitled, "The Global Economic Impacts Association with Virtual and Augmented Reality", estimating the potential economic impacts of Augmented Reality and Virtual Reality (AR and VR) technologies on behalf of Facebook. The authors developed a production model calculating the per unit dynamic contribution of smartphones and tablets and then used the results as a baseline comparator for making forecasts for AR and VR devices. The results revealed a $11,262 lifetime contribution over 5 years for each smartphone and tablet to US GDP and a 4.3 multiplier on direct expenditure (see Appendix B for full regression results from the study). While the research utilized this model for AR and VR devices, rather than expanding upon smartphones and tablets, this paper has applied it to existing data from other sources.

The second and third primary sources of data are from two reports from the Pew Research Center (Anderson, 2015; Smith, 2015) and one from the National Research Council (Lucky and Eisenberg, 2006). The Pew reports provided usage statistics and penetration rates for smartphones and tablets among the US population, which could then be applied to US Census data. These find that approximately 68% of US adults possessed a smartphone and that approximately 45% of US adults possessed a tablet in 2015. The National Research Council report provided data on the Gross Domestic Income (GDI) contributions of the traditional telecommunications sector – both for the hardware and services – in 2003 before the introduction of smartphones. The study calculated that the telecoms sector contributed approximately 3.0% of GDI in the United States in 2003 with approximately 2.6% coming from services and 0.4% coming from hardware.

Using these and some basic assumptions, this paper calculates there were approximately 274 million smartphones and tablets in the United States in 2015 and calculates a 0.85 to 0.15 split between services and hardware in the traditional telecoms sector prior to smartphone introduction. It then applies the per unit GDP contribution estimates from the Analysis Group regression model to these, yielding a 3.11% GDP contribution for mobile internet and apps. Table 2 summarizes these calculations.

The calculation summarized in Table 2 requires some verification,[2] but there is reason to believe that the estimate is solid. It draws on findings from robust research studies and is in-line with the figures estimated for the internet sector as a whole and for other comparable sectors such as telecommunications. Even if we assume an overly conservative contribution split from mobile internet and app services to the US

[2] It makes the following assumptions: 1) that there was the same ratio of GDP contribution between hardware and services in telecoms in 2003 as there was for the GDI contribution; 2) the same ratio between hardware and services existed in the smartphone and tablet industry in 2015 as existed in pre-smartphone era telecoms sector; and 3) that the services of the smartphone and tablet markets all incorporate mobile internet and apps in some way.

Table 2 / The economic contribution of mobile internet and app services to the US economy	
Number of US adults	242,470,820
% of adult population with smartphones	0.68
% of adult population with tablets	0.45
Estimated number of smartphones in USA	164,880,158
Estimated total tablets and smartphones	109,111,869
Estimated total tablets and smartphones	273,992,027
GDP contribution Per Unit from regression (cumulative over 5 year period)	$11,262
Estimated GDP contribution from Tablets and Smartphones	$3,085,698,203,569
Per year GDP contribution	$617,139,640,714
US GDP Annual	$16,770,000,000,000
% of GDP from smartphones and tablets	0.0368
Conservative GDP contribution assumption (50% of value from internet and app usage)	0.50
GDP contribution assumption based on traditional telecoms contributions (84.6% of value from mobile internet and app usage)	0.85
Conservative GDP contribution of mobile internet and apps to US GDP	1.84%
US GDP of contribution of mobile internet and apps (based on historic telecoms contributions)	3.11%
GDP Contribution Determination	
Value-added assumption for traditional telecoms services	2.60%
GDI Contribution for traditional telecoms hardware	0.40%
Ratio of GDI contribution from hardware vs services	0.1538

Source: Author's elaboration; Information from: Lucky and Eisenberg (2006); Anderson (2015); Smith (2015); Christensen et al. (2016)

**The telecommunications industry is a major direct contributor to U.S. economic activity. The U.S. Census Bureau estimates that just over 3 percent of the U.S. gross domestic income (GDI) in 2003 was from communications services (2.6 percent) and communications hardware (0.4 percent)—categories that are narrower than the broad definition of telecommunications offered above. At 3 percent, telecommunications thus represented more than a third of the total fraction of GDI spent on information technology (IT; 7.9 percent of GDI) in 2003. (Lucky and Eisenberg, 2006: 8). 2006. Robert W. Lucky and Jon Eisenberg, Editors; Committee on Telecommunications Research and Development; Computer Science and Telecommunications Board; Division on Engineering and Physical Sciences; National Research Council*

economy (say 50% with the other 50% of value coming from their manufacture and non-internet related services), the contribution of mobile internet and app services remains at a substantial 1.84%. Most importantly, these figures demonstrate that we are overdue for a new approach to segmenting and measuring the internet economy.

Section D /

Beginning the Conversation

The particulars of that segmentation are too large to detail here, but the paper generally proposes an update of existing industrial classification systems in two ways. The first is to create a new primary classification code (along with a full set of subsector classifications) for services and products that are offered exclusively through internet platforms. Two examples are mobile games that can only be played through an internet connection on a mobile device and web services such as cloud hosting. The second change is to add two unique sub-classifications to each existing industrial subsectors for 1) direct provision of traditional services and products through the internet (such as online purchases from a retail store as a sub-classification of the NAICS "Retail Trade" sector) and 2) new products and services that draw on traditional sectors offered through new and unique internet platforms (such as a ride-sharing services as a sub-classification of the NAICS "Transportation and Warehousing").

The value of this approach lies in its recognition of the internet as a unique type of sector. Not only does the internet provide completely new and unique products and services that have only come into existence in the past decade, it also provides every other traditional product and service a medium for improved productivity. Some have labeled it as a new type of public good, others as a type of infrastructure, and other as a general purpose technology. There is truth in all of these, but they also oversimplify; the internet is singular in potential applications and should be considered correspondingly.

Of course, these changes are not easy to implement, but they are necessary and overdue. Until we change our approach to classifying and understanding the internet as an economic sector, we will continue to underestimate its impact. The Internet's rapidly growing contribution to both domestic GDP and the economy presented in Table 1 demonstrates the scale of this necessity, and the multiple subsectors, such as the mobile internet and app services presented in Table 2, detail the variety and complexity of these contributions. Traditional approaches to conceptualizing the Internet miss many of its economic contributions to our society. Put differently, we are looking at the wrong places and at the wrong things. Until we refocus, policymakers, regulators, and the general public will continue to misunderstand the role of the internet.

Section E /

Conclusion

A typical child born today will have no outstanding memory of the internet, yet he or she will develop an intuition for the internet because it will be such an integral part of life. Simply look at the ease with which a child interacts with an educational app on their parent's tablet, swiping and clicking through systems that did not exist two years ago. Now compare that image to your own experience of trying to figure out how to use Snapchat or your parents' experience learning about trending topics. The learning curve may have been sharp for some, but it is universally flattening.

As the internet flattens traditional barriers, we must refresh how we understand the internet in the economy. We must improve how we conceptualize it and, subsequently, how we classify its various components. The internet comprised 6% of the US GDP in 2014 and it is growing rapidly. Mobile internet and app services, just one of its subsectors, comprised over 3% of US GDP in 2015 and continues to create new products and services previously unimagined. Still our research, policies, and regulatory perspectives lag behind. It's time to update our approach so we can begin to fully appreciate the profound economic potential of the internet.

References

Anderson, Monica. (2015). "Technology Device Ownership: 2015". Pew Research Center. Washington, DC. Available from: http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/

Center for Automotive Research. (2015). "Contribution of the Automotive Industry to the Economies of All Fifty States and the United States." Prepared by Kim Hill, Debra Menk, Joshua Cregger, and Michael Schultz. Alliance of Automobile Manufacturers. Ann Arbor, Michigan. Available from: http://www.autoalliance.org/files/dmfile/2015-Auto-Industry-Jobs-Report.pdf

Christensen, Laurits R., Wes Marcik, Greg Rafrert, and Carletta Wong. (2016). "The Global Economic Impacts Associated with Virtual and Augmented Reality". White paper. Analysis Group, Inc. Available from: http://www.analysisgroup.com/uploadedfiles/content/insights/publishing/analysis_group_vr_economic_impact_report.pdf

Dean, David, Sebastian Digrande, Dominic Field, Andreas Lundmark, James O'Day, John Pineda, and Paul Zwillenberg. (2012). "The Internet Economy in the G-20: The $4.2 Trillion Growth Opportunity." The Connected World. BCG Report. The Boston Consulting Group. Available from: https://www.bcgperspectives.com/content/articles/media_entertainment_strategic_planning_4_2_trillion_opportunity_internet_economy_g20/

du Rausas, Matthieu Pélissié, James Manyika, Eric Hazan, Jacques Bughin, Michael Chui, and Remi Said. (2011). "Internet matters: The Net's sweeping impact on growth, jobs, and prosperity." McKinsey Global Institute, McKinsey & Company. Available from: http://www.mckinsey.com/industries/high-tech/our-insights/internet-matters

Koutroumpis, P. (2009). "The Economic Impact of Broadband Growth: Why and For Whom?". NBER Working Paper No. 7591. National Bureau of Economic Research. Cambridge, MA.

Lucky, Robert W. and Jon Eisenberg, eds., (2016). Renewing U.S. Telecommunications Research. National Research Council of the National Academies, Committee on Telecommunications Research and Development. Washington, D.C.: The National Academies Press. Available from: http://www.nap.edu/catalog/11711/renewing-us-telecommunications-research

OECD. (2008). The Seoul Declaration for the Future of the Internet Economy, Ministerial session. 18 June 2008. Available from: https://www.oecd.org/sti/40839436.pdf

OECD. (2013). "Measuring the Internet Economy: A Contribution to the Research Agenda". OECD Digital Economy Papers, No. 226, OECD Publishing. Available from: http://dx.doi.org/10.1787/5k43gjg6r8jf-en

Smith, Aaron. (2015). "U.S. Smartphone Use in 2015." Pew Research Center. Washington, DC. Available from: http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/

Siwek, Stephen F. (2015). "Measuring the U.S. Internet Sector". Internet Association. Washington, DC. Available from: http://internetassociation.org/wp-content/uploads/2015/12/Internet-Association-Measuring-the-US-Internet-Sector-12-10-15.pdf

The World Bank. (2012). World Development Indicators. Washington, D.C.: The World Bank (producer and distributor). Available from: http://data.worldbank.org/data-catalog/world-development-indicators

Appendix A / Comparing the internet sector with traditional NAICS sectors

Line		2012	2013	2014	2015	2015 Rank
1	Gross domestic product	100	100	100	100	na
2	Private industries	86.4	86.6	86.9	87.1	**1**
101	services-producing Private industries [2]	66.8	66.8	67.1	68.2	2
54	Finance, insurance, real estate, rental, and leasing	20.0	19.8	20.0	20.3	3
100	Private goods-producing industries [1]	19.6	19.9	19.8	18.9	4
60	Real estate and rental and leasing	12.9	12.9	13.0	13.2	**5**
90	Government	13.6	13.4	13.1	12.9	**6**
65	Professional and business services	11.8	11.7	11.9	12.2	**7**
12	Manufacturing	12.3	12.2	12.1	12.1	**8**
61	Real estate	11.8	11.8	11.9	12.0	**9**
62	Housing	9.6	9.5	9.6	9.6	**10**
96	State and local government	9.2	9.1	9.0	8.9	**11**
74	Educational services, health care, and social assistance	8.3	8.2	8.2	8.3	**12**
97	General government	8.4	8.3	8.2	8.1	**13**
76	Health care and social assistance	7.1	7.1	7.1	7.2	**14**
55	Finance and insurance	7.1	6.9	7.0	7.1	**15**
66	Professional, scientific, and technical services	7.0	6.8	6.9	7.1	**16**
13	Durable goods	6.5	6.5	6.5	6.5	**17**
34	Wholesale trade	6.0	6.0	6.0	6.0	**18**
102	Information-communications-technology-producing industries [3]	5.7	5.9	5.9	…	**19**
35	Retail trade	5.8	5.8	5.8	5.8	**20**
	INTERNET SECTOR	**5.54**		**6.0**		**21**
25	Nondurable goods	5.8	5.7	5.6	5.5	**22**
49	Information	4.6	4.8	4.8	4.8	**23**
69	Miscellaneous professional, scientific, and technical services	4.2	4.1	4.2	4.3	**24**
91	Federal government	4.4	4.3	4.1	4.1	**25**
11	Construction	3.6	3.7	3.8	4.0	**26**
82	Arts, entertainment, recreation, accommodation, and food services	3.7	3.8	3.8	3.9	**27**
92	General government	4.1	4.0	3.9	3.8	**28**
77	Ambulatory health care services	3.4	3.4	3.4	3.5	**29**
	MOBILE INTERNET AND APPS				**3.11**	**30**
71	Administrative and waste management services	3.0	3.0	3.0	3.1	**31**

Appendix A / Comparing the internet sector with traditional NAICS sectors

Line		2012	2013	2014	2015	2015 Rank
39	Other retail	3.0	3.0	3.0	3.1	**32**
78	Hospitals and nursing and residential care facilities	3.1	3.1	3.0	3.1	**33**
40	Transportation and warehousing	2.9	2.9	2.9	2.9	**34**
86	Accommodation and food services	2.7	2.8	2.8	2.9	**35**
72	Administrative and support services	2.7	2.7	2.8	2.9	**36**
56	Federal Reserve banks, credit intermediation, and related activities	3.0	2.9	2.8	2.8	**37**
58	Insurance carriers and related activities	2.5	2.5	2.6	2.6	**38**
52	Broadcasting and telecommunications	2.3	2.4	2.4	2.4	**39**
63	Other real estate	2.2	2.3	2.3	2.4	**40**
79	Hospitals	2.3	2.3	2.2	2.3	**41**
89	Other services, except government	2.2	2.2	2.2	2.2	**42**
93	National defense	2.5	2.4	2.3	2.2	**43**
32	Chemical products	2.1	2.1	2.1	2.1	**44**
88	Food services and drinking places	1.9	2.0	2.0	2.1	**45**
70	Management of companies and enterprises	1.9	1.9	1.9	2.0	**46**
6	Mining	2.5	2.6	2.6	1.7	**47**
10	Utilities	1.6	1.6	1.6	1.6	**48**
19	Computer and electronic products	1.6	1.6	1.5	1.6	**49**
68	Computer systems design and related services	1.4	1.4	1.4	1.5	**50**
94	Nondefense government	1.6	1.6	1.5	1.5	**51**
26	Food and beverage and tobacco products	1.4	1.4	1.4	1.4	**52**
57	Securities, commodity contracts, and investments	1.4	1.3	1.4	1.4	**53**
67	Legal services	1.4	1.3	1.3	1.3	**54**
50	Publishing industries, except internet (includes software)	1.2	1.2	1.2	1.2	**55**
3	Agriculture, forestry, fishing, and hunting	1.2	1.4	1.2	1.1	**56**
75	Educational services	1.1	1.1	1.1	1.1	**57**
36	Motor vehicle and parts dealers	1.0	1.0	1.0	1.1	**58**
64	Rental and leasing services and lessors of intangible assets	1.1	1.1	1.1	1.1	**59**
83	Arts, entertainment, and recreation	1.0	1.0	1.0	1.0	**60**
7	Oil and gas extraction	1.7	1.8	1.7	1.0	**61**
4	Farms	0.9	1.1	1.0	0.9	**62**
18	Machinery	0.9	0.9	0.9	0.9	**63**

Appendix A / Comparing the internet sector with traditional NAICS sectors

Line		2012	2013	2014	2015	2015 Rank
21	Motor vehicles, bodies and trailers, and parts	0.8	0.8	0.8	0.9	**64**
31	Petroleum and coal products	1.1	1.0	1.0	0.9	**65**
37	Food and beverage stores	0.9	0.9	0.9	0.9	**66**
17	Fabricated metal products	0.9	0.8	0.8	0.8	**67**
38	General merchandise stores	0.9	0.8	0.8	0.8	**68**
44	Truck transportation	0.8	0.8	0.8	0.8	**69**
80	Nursing and residential care facilities	0.8	0.8	0.8	0.8	**70**
87	Accommodation	0.8	0.8	0.8	0.8	**71**
22	Other transportation equipment	0.7	0.7	0.7	0.7	**72**
47	Other transportation and support activities	0.6	0.6	0.6	0.7	**73**
51	Motion picture and sound recording industries	0.7	0.7	0.7	0.7	**74**
98	Government enterprises	0.7	0.8	0.7	0.7	**75**
81	Social assistance	0.6	0.6	0.6	0.6	**76**
84	Performing arts, spectator sports, museums, and related activities	0.5	0.5	0.5	0.6	**77**
24	Miscellaneous manufacturing	0.5	0.5	0.5	0.5	**78**
41	Air transportation	0.5	0.5	0.5	0.5	**79**
53	Data processing, internet publishing, and other information services	0.4	0.5	0.5	0.5	**80**
85	Amusements, gambling, and recreation industries	0.4	0.5	0.5	0.5	**81**
8	Mining, except oil and gas	0.5	0.5	0.5	0.4	**82**
33	Plastics and rubber products	0.4	0.4	0.4	0.4	**83**
9	Support activities for mining	0.4	0.4	0.4	0.3	**84**
15	Nonmetallic mineral products	0.2	0.3	0.3	0.3	**85**
16	Primary metals	0.4	0.3	0.3	0.3	**86**
20	Electrical equipment, appliances, and components	0.3	0.3	0.3	0.3	**87**
29	Paper products	0.3	0.3	0.3	0.3	**88**
42	Rail transportation	0.3	0.3	0.3	0.3	**89**
48	Warehousing and storage	0.3	0.3	0.3	0.3	**90**

Source: Value Added by Industry as a Percentage of Gross Domestic Product

Appendix B / Regression Results Showing Per Unit GDP Per Capita Contributions of Smartphones and Tablets								
Independent Variables	**1**		**2**		**3**		**4**	
Smartphone + Tablet Units Shipped (MM)	14,370	***	11,737	***	11,782	***	11,262	***
Enrolled in Primary Schooling (%)	-		2,329		4,277		7,926	
Enrolled in Secondary Schooling (%)	-		4,707		5,221		4,692	
Fertility Rate Adjusted for Child Mortality	-		560,483		656,580		518,703	
Government Expenditure (% GDP)	-		(14408)		(19,783)		(10,349)	
Gross Capital Formation (% GDP)	-		5,947		6,734		9,211	
Inflation, Consumer Prices (%)	-		(2615)		(2,847)		(3,141)	
Rule of Law Index	-		178,640	***	162,580	*	188,500	**
Total Population (MM)	-		28,528	***	28,952	***	27,849	***
Patent Applications per Capita	-		-		(20,686,010)		42,178,820	
Broadband Subscribers per 100 people	-		-		-		14,257	*
Constant	1,041,898	***	(2,897,555)	***	(3,251,124)	*	(3,481,985)	*
# Observations	532		405		367		342	
Adjusted R^2	0.66		0.78		0.78		0.80	

Source: Table recreated from "The Global Economic Impacts Associated with Virtual and Augmented Reality." by Christensen et al. (2015: 16). Whitepaper. (Commissioned by Facebook). Analysis Group.

Notes:

[1] GDP ($MM) is in millions of constant 2014 international dollars representing purchasing power parity. This variable is calculated using "GDP (constant local currency ("LCU")), "GDP (current LCU)," and "PPP conversion factor, GDP (LCU per international $)," with 2014 as the base year.

[2] All specifications are fixed effect models, to account for both country and year effects.

*[3]*** represents statistical significance at the 1% level. ** represents statistical significance at the 5% level. * represents statistical significance at the 10% level.*

[4] Number of observations vary between models due to specification differences and data availability.

Sources: The World Bank, World Development Indicators, October 14, 2015, available at: http://data.worldbank.org/data-catalog/world-development-indicators; The World Bank Group, Worldwide Governance Indicators, October 2015, available at: http://info.worldbank.org/governance/wgi/index.aspx#home; Strategy Analytics, :"Q3 2015: Tablet Operating System Forecast - Shipments, Installed Base & by Price Tier 2010 - 2019," August 2015.

Internet Association is the only trade association that exclusively represents leading global internet companies on matters of public policy. The association's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. The internet creates unprecedented benefits for society, and as the voice of the world's leading internet companies, Internet Association ensures stakeholders understand these these benefits.

www.internetassociation.org

Published on *NTIA* (https://www.ntia.doc.gov)

Twenty Years after the Birth of the Modern Internet, U.S. Policies Continue to Help the Internet Grow and Thrive

May 01, 2015 by John Morris

Yesterday, I had the great opportunity to speak at the United States Telecommunications Training Institute [1] (USTTI) to a group of foreign government officials focused on Internet and cybersecurity issues. My talk focused on how NTIA sees the role of the Internet in the U.S. economy, and what key policies have contributed to the strength of the U.S. Internet economy.

Participants included representatives from Bangladesh, Barbados, Benin, Botswana, Burkina Faso, Ecuador, Ethiopia, Ghana, Senegal, Sri Lanka, Tanzania and Uganda. The daylong course [1], organized by NTIA's Office of International Affairs, introduced basic concepts in Internet policymaking and governance to build awareness, and develop and improve policymaking skills while working in a multistakeholder environment with government, civil society, industry and others. The course, which will take place again in September, examined U.S. Internet policy approaches, taking into consideration some of the key international issues and debates occurring globally.

Our discussion happened to fall on the 20th birthday of the commercial Internet, which fit right into my theme. The NSFnet was decommissioned on April 30, 1995, paving the way for the commercial use and private governance of the Internet. In its wake, we have witnessed an extraordinary explosion of innovation and economic growth in the online environment.

These are six key policies that I believe have contributed to the strength of the U.S. digital economy and provide a model for developing countries, such as those that participated in the USTTI course, to consider as they seek to grow their economies:

- Trusting the Private Sector: This is particularly powerful as we are celebrate the 20th anniversary of the U.S. decision to take a network it had originated and trust it to the private sector to innovate and take the Internet to the next level. NTIA has long been involved in encouraging the Internet community - working through multistakeholder processes - to move forward with great ideas.
- Connecting Users: The U.S. government has invested heavily in supporting broadband access and penetration with a range of programs aimed at supporting the deployment of broadband. NTIA's BroadbandUSA [2] is an initiative to support community broadband projects and to promote broadband deployment and adoption.
- Empowering Users: U.S. policies have empowered users to access knowledge, communicate, express their opinions and launch small businesses to reach global audiences.

- Protecting Platforms: U.S. law provides strong protections for online platforms from undue interference and regulation. A critical example of U.S. law is "Section 230 [3]" of the Communications Act as amended in 1996, which protects online platforms against claims arising from hosting information posted by users and other third parties.
- Strong and Balanced Intellectual Property Regime: The United States is dedicated to the protection of intellectual property to foster and protect creativity. The United States supports a balanced approach to intellectual property that includes an emphasis on enforcement and protection but also recognizes limitations and "fair use."
- Reliance on Multistakeholder Policy Approaches: Throughout all of our work, we have looked to multistakeholder consensus-based processes to keep the Internet and its innovation moving forward. NTIA, working with other parts of the Department of Commerce through the Internet Policy Task Force, has supported multistakeholder efforts focused on the domain name system, privacy, intellectual property and cybersecurity. To help preserve the multistakeholder approach to Internet governance, NTIA last year announced [4] it would transition our stewardship role over key functions related to the Internet's domain name system to the global multistakeholder community. NTIA Administrator Lawrence E. Strickling earlier this week reiterated [5] why we believe this is the best way to ensure the Internet continues to grow and thrive.

These policies have contributed to unprecedented economic growth and security in the United States, and led to breakthroughs across national priorities from health care, education and energy. We are excited to see what the Internet, and the free flow of information across it, will spur in the coming years.

Topics:
Internet Policy [6]

National Telecommunications and Information Administration
1401 Constitution Ave., NW Washington, DC 20230

Source URL: https://www.ntia.doc.gov/blog/2015/twenty-years-after-birth-modern-internet-us-policies-continue-help-internet-grow-and-thriv#comment-0

Links
[1] http://ustti.org/courses/display.php?CourseID=8
[2] http://www2.ntia.doc.gov/
[3] http://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/html/USCODE-2011-title47-chap5-subchapII-partI-sec230.htm
[4] http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions
[5] https://www.ntia.doc.gov/speechtestimony/2015/remarks-assistant-secretary-strickling-internet2-global-summit
[6] https://www.ntia.doc.gov/category/internet-policy

INNOVATION ECONOMY

How Effective Internet Policy Can Support Startups

Testimony before the House Ways & Means Subcommittee on Trade

July 13, 2016

Hearing on Expanding U.S. Digital Trade and Eliminating Barriers to U.S. Digital Exports

Kavita Shukla
Founder and CEO
Fenugreen FreshPaper

1. About Fenugreen FreshPaper

Good morning. Chairman Reichert, Ranking Member Rangel, and members of the Committee, thank you for the opportunity to be here today.

My name is Kavita Shukla. I'm the founder and CEO of Fenugreen FreshPaper, a social enterprise taking on global food waste with a simple innovation.

Five years ago, I set up a stall at my local farmer's market with the hope of helping my local community have greater access to fresh, healthy produce. I never could have imagined that within a few months, my idea would be shared across the globe, and that one day, my invention would land on the shelves of some of the largest retailers in the world -- from Whole Foods to Walmart. I'm here to share the story of how accessing global markets made all of this possible.

This was my idea: FreshPaper, a simple piece of paper infused with organic spices that keeps fruits & vegetables fresh for up to 2-4 times longer. A simple, sustainable solution to the massive global challenge of food waste.

FreshPaper began as a middle-school science project, inspired by my grandmother. After immigrating to the United States with my family as a child, I returned to visit my grandparents in India, and accidentally drank some unfiltered tap water. My grandmother gave me a homemade mixture of spices as remedy, and I ended up not getting sick. That experience sparked my curiosity, and when I got back home to Maryland, I was inspired to start a science project to learn more about the spices my grandmother used. After tinkering around in my garage with jars of dirty pond water and spices, I discovered that some of the spices seemed to stop the growth of bacteria and fungus.

One day, after seeing moldy strawberries while grocery shopping with my mom, I wondered if my spice mixture could keep produce fresh for longer. To make a long

story short, after spending most of high school meticulously rotting fruits and vegetables, I created FreshPaper.

FreshPaper ended up winning a 1st place award at the Intel International Science Fair, and I was a senior in high school when I was issued a patent for FreshPaper. It was an unlikely outcome to my story, possible only in this country – my grandmother with all of her brilliance never had the opportunity to pursue her ideas, and at 17, I had a patent and was on my way to Harvard to pursue mine.

I was so excited about how FreshPaper could help people like my grandmother in areas like the village where she was from, and I couldn't wait to get my invention out into the world. I learned that, while the world's farmers harvest enough food to feed the planet, almost 800 million people go hungry every day,[1] and that over 1 billion people live without access to refrigeration.[2] FreshPaper, I believed, could help address global food waste and hunger.

As soon as I got to college, I set out to build a non-profit, and ended up learning how hard it can be to give something away for free. After trying and failing over and over, my friends and advisers suggested that I consider a more "realistic" career path. Like many aspiring entrepreneurs, I was told that I needed more experience, more degrees, more money – more than I had, and more than I was. So I gave up.

In the summer of 2011, more than a decade after I first started working on my science project, I decided to give my idea, and myself, one last chance.

I stayed up all night making a batch of FreshPaper by hand in the kitchen of my tiny studio apartment, and early Saturday morning, a friend and I set up a stall at our local farmer's market in Cambridge, Massachusetts. We stood in the street handing out sheets to passersby.

In the weeks and months that followed, we were amazed by the response. People started telling us, "FreshPaper makes it possible for me to afford feeding my family fresh fruits and vegetables." As I began to realize that my small sheet of paper was having an impact on our local food system, I was inspired to think bigger.

---

[1] United Nations Food and Agriculture Organization, International Fund for Agricultural Development, World Food Programme, *The State of Food Insecurity in the World 2015. Meeting the 2015 international hunger targets: taking stock of uneven progress*. Rome, FAO.

[2] International Energy Agency, *Key World Energy Statistics 2015.* OECD/IEA 2015

2. About our global journey

We created a very basic online store, and on a whim, we enabled international markets. In less than a minute, FreshPaper was available worldwide. While we were selling FreshPaper in just one local store, the Harvest Co-Op, we were shipping FreshPaper across the world to places like Spain, Australia, Canada, the UK, Indonesia, Japan, and Brunei.

I now joke that that we went global by accident. With just a few errant clicks, my farmer's market stand now had access to an almost infinite global market.

Of course, we had no idea how to ship globally – at the time, we didn't even know how to make a pallet. But at every roadblock, we Googled our way out, and through trial and error found digital tools to make our global business a reality. We found out that PayPal could enable us to collect foreign payments and convert currencies, that Intuit Quickbooks could help us keep track of our earnings, and discovered that UPS Mail Innovations simplified the customs process.

We had started with less than a $1000 – we had no outside funding, no marketing budget, and no experience. But within a few months, we were carting wheelbarrows of orders to our local post office, and shipping our made in the USA product to places I could never have imagined. Those international orders helped keep our fledgling business alive, giving us time to build our customer base locally.

Once we started shipping out these international orders, FreshPaper started to be featured by newspapers and media outlets around the globe. I was invited to speak about FreshPaper in Japan, Denmark, France, the UK, and Switzerland. I found myself addressing the World Trade Organization in Geneva, and on stage with Sir Richard Branson at the Global Entrepreneurship Congress in Liverpool.

FreshPaper even won the world's largest prize for design (the INDEX: Design to Improve Life Award), previously awarded to Apple and Tesla, which provided us with a crucial 100,000 euro prize that helped us scale our production. Last summer, FreshPaper became the first product ever to be launched globally by Amazon as part of Amazon Launchpad, a program designed for startups, making our simple idea available in 180 countries overnight. The Internet took our farmer's market stand global.

Today, FreshPaper is made in factories in the Midwest and Maryland, and we're working with international distributors to launch in retailers across the globe, and to reach more farmers and families worldwide. We've seen the power of international markets. We are here today because of an open global Internet. But the excessive costs, paperwork, and logistics to access these global markets are still challenges that we and other entrepreneurs face every day.

3. The role of government policy in eliminating barriers to digital exports

I'm here because I believe we must reduce barriers to unleash our country's entrepreneurial talents, innovations, and energy, and encourage small business owners to think global from day one.

My story is not unique. Nor should it be. I often think of the jam-seller who set up a stall at her local farmer's market. The single mom I met who was making ends meet by selling items on eBay. The young programmer dreaming up the next big app. Entrepreneurs across this country drive our economy with their ingenuity, with their grit, with their optimism, and with their success.

But we cannot do it alone.

We are happy to work hard, to hustle, to spend sleepless nights figuring out how to make the impossible a reality, to push through the resistance, the naysayers, and the doubt – and, in the unlikely event of our success, share the benefits with our communities, create American jobs, build factories, and design organizations that will outlive us.

We need your help.

Ensure that an open, global Internet is available so that our partners, customers and community from around the world can connect with us, and so that we can use technology to operate our business on a global basis. Utilize trade agreements and other platforms to reduce tariffs on the products we make, and to simplify customs procedures. Help entrepreneurs like me understand the resources that the U.S. Government has for startups looking to take their business global.

Give us access and reduce barriers to the spread of our ideas, and we'll work hard to figure out the rest.

Thank you so much for the opportunity to testify.

- **Big Data:** Big data is the collection and analysis of large and complex data sets. This term is often described by the "Three V's" – volume, variety, and velocity. These qualities are important to understanding that this term not only applies to large data sets collected by one entity, but also combined data from multiple sources and the speed and quality of analysis it undergoes. Government agencies and businesses collect data from multiple sources, including: social media profiles, online comments and forum posts, computer and mobile device log files, cloud applications, and archived documents such as insurance forms and customer correspondence.
- **Biometrics:** Technology that identifies you based on your biological or behavioral traits (e.g. fingerprinting, facial recognition, genetic testing, or iris scanning). It is often used for security purposes but can also be used for surveillance.
- **Bulk Collection:** The government's practice of collecting massive amounts of data belonging to large groups of people in a generally indiscriminate manner. The National Security Agency intercepts over a billion people's telephone and Internet communications worldwide. Advocates are concerned about the amount of data collected and how the government uses this data.
- **Cybersecurity:** Measures taken to protect the security of computers and computer networks.
- **Data security:** Measures taken to protect the confidentiality, integrity, and availability of data.
- **Do Not Track:** A technical Web standard maintained by the World Wide Web Consortium; a feature in certain web browsers that allows users to let websites know that they would like to opt-out of third-

party tracking. Third party companies collect web users' personal information and online activities for a variety of purposes, including behavioral advertising.

- **Fair Use:** Doctrine in American copyright law that permits limited use of copyrighted material. People using copyrighted materials for parody, news reporting or research often do not have to acquire permission from the rights holders.
- **Federal Communications Commission (FCC):** An independent U.S. government agency overseen by Congress that regulates interstate and international communications by radio, television, wire, satellite and cable.
- **Federal Trade Commission (FTC):** An independent U.S. government agency that protects consumers and eliminates anticompetitive business practices.
- **Section 702 of the FISA Amendments Act (2008):** Authorizes surveillance of people believed to be located outside the U.S. who are not U.S. citizens.
- **Gag Orders:** An order from courts or government agencies that restricts recipient companies from sharing information with the public or third parties.
- **Intermediary Liability:** When private companies are held responsible for what their users say and do online. In the U.S., there are strong protections for intermediaries from liability for their users' speech. Holding intermediaries legally responsible for what their users post can be used by governments to suppress dissent and limit intermediaries' willingness to host lawful speech.
- **International Telecommunications Union (ITU):** This is the United Nations' specialized agency for information and communication technologies. They allocate global radio spectrum and satellite orbits, develop the technical standards that ensure networks and technologies seamlessly interconnect, and work to improve access to technologies in underserved communities worldwide.
- **Internet Corporation for Assigned Names and Numbers (ICANN):** ICANN is the nonprofit organization that coordinates the Internet's

global domain name and addressing system.

- **Internet of Things:** Chips, transmitters, sensors, and other networking components placed in real-world objects or animals that can transmit data for a network. Examples include a heart monitor implant, a farm animal with a biochip transponder, or home appliances that can be programmed to learn your preferences and can be controlled remotely.
- **Metadata:** Metadata – technically, data about data – provides information about the records created or stored by a computer or telecommunications device. It can include how the data was created, the purpose of the data, the time and date the data was created, the creator or author of the data, numbers dialed to or from a device, and the location on a computer network where the data was created.
- **National Security Administration (NSA):** The U.S. intelligence agency responsible for global monitoring, collection, decoding, translation and analysis of information and data for foreign intelligence and counterintelligence purposes.
- **National Security Letters (NSL):** The FBI can issue an NSL to collect bank, telephone company, and Internet Service Provider customer records. Companies are required to comply with NSL requests and are prohibited by a gag order from telling customers when they receive these letters.
- **National Telecommunications and Information Association (NTIA):** An executive branch agency within the Department of Commerce that advises the president on telecommunication and Internet policy issues.
- **Net Neutrality:** The principle that Internet Service Providers and governments should treat all data on the Internet equally, by not prioritizing network traffic or charging different prices.
- **Online Behavioral Advertising (OBA):** Companies collect information about a person's online activity and use it to tailor ads or content.
- **Privacy by Design:** An approach to engineering, design or business plans that takes user privacy into account from the beginning and embeds it throughout the whole product development process.

- **Privacy Policy:** A statement or legal document that discloses the ways a party gathers, uses, discloses and manages a customer or client's data.
- **Right to be Forgotten:** The idea that an individual has the right to remove public information about themselves from the Internet, or to petition search engines not to list certain links to publicly available information in search results. Following a ruling from the Court of Justice for the European Union, the scope of this right is being explored in Europe, but faces skepticism in the United States because of its conflict with First Amendment principles.
- **Safe Harbor:** The data transfer agreement between the U.S. and EU recently struck down in the *Schrems* decision.
- **Section 512 of the Copyright Act (Safe Harbor):** A provision of The Digital Millennium Copyright Act which protects Internet Service Providers from the consequences of their users' actions, such as copyright infringement.
- **Section 215 of the Patriot Act:** Allows the government to obtain secret court orders to collect "tangible things" that could be relevant to a government investigation, such as books, records, papers and documents.
- **Subpoena:** When a prosecutor or government agency requires someone to testify or produce evidence – typically without seeking approval from a neutral third party like a judge.
- **Warrant:** A document issued by a judicial or government official authorizing the police or some other body to make an arrest or search premises.
- **Upstream Collection:** A term to describe the NSA's tactic for intercepting telephone and Internet traffic as it flows through major Internet cables and switches.

Legislation

Privacy Protection

Fair Credit Reporting Act (FCRA): The FCRA was enacted in 1970 to promote accuracy, fairness and the privacy of personal information assembled by Credit Reporting Agencies, including requiring consumer protections for credit reports, consumer investigatory reports and employment background checks. Typically, consumer credit reports contain information on financial accounts, and include credit card balances and mortgage information. In addition to compiling traditional consumer credit reports, companies are now also creating social media reports, which are supplied to employers as part of employment screenings. In May 2011 the FTC confirmed that employers must comply with the requirements of FCRA when using public information furnished by Internet and social media background screening services.

Family Educational Rights and Privacy Act (FERPA): This law was enacted in 1974 and protects the privacy of student education records. It gives parents the right to review a student's educational records and request corrections when the parent believes records are inaccurate or misleading. The law also requires, with a few exceptions, a school to have written permission from a parent before releasing a student's educational record to other parties.

Privacy Act of 1974: The Privacy Act of 1974 requires government agencies to show people any records kept on them. It also requires government agencies to follow "fair information practices" when gathering and handling personal data and places restrictions on how agencies can share an individual's data with other people and agencies. It allows individuals to sue the government for violating these provisions.

Electronic Communications Privacy Act (ECPA): ECPA was passed in 1986 to expand and revise federal wiretapping and electronic eavesdropping provisions. It was envisioned to create "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement," but it allows law enforcement warrantless access to any email after 180 days.

Video Privacy Protection Act: Congress passed the Video Privacy Protection Act of 1988 to prevent the disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual material." The Act is not often invoked, but stands as one of the strongest protections of consumer privacy against a specific form of data collection.

Health Insurance Portability and Accountability Act (HIPAA): HIPAA regulates when and how health information about individuals in the United States may be disclosed. The law offers some rights to patients, such as the ability to view and correct medical records, but its capacity to protect disclosures of patient medical information is limited, as the law only applies to health care providers, health plans, healthcare clearinghouses, and relevant business associates of these entities. While the law covers health information technology and electronic healthcare records, it does not apply to many entities that collect and use health information from individuals, such as mobile applications, wearable device companies, or genetic testing services. When non-HIPAA covered entities collect and use personal health information for internal purposes like research and development, these activities are also unregulated but they may be informed by laws such as the Common Rule, which sets ethical guidelines for how government-funded entities may gather and use information from human subjects. Ethical considerations should be a part of any use of data generated by human subjects, including the users of health apps or devices. Though the Common Rule only applies to federally-funded research, companies may find the law's detailed ethical guidance useful, including ways of obtaining and documenting informed consent and regulations on implementing special protections for data from minors and/or the disabled.

Children's Online Privacy Protection Act (COPPA): COPPA was enacted in 1998 to regulate online data collection from children under the age of 13. It requires websites to post clear and comprehensive online privacy policies and get consent from parents before collecting children's personal information. Websites must also establish procedures that protect the

confidentiality, security, and integrity of the personal information collected, including persistent identifiers used to recognize a user over time and across different websites, such as cookies.

Email Privacy Act: In March 2013, a bipartisan coalition of Congressmen introduced the Email Privacy Act to reform ECPA. The bill would ensure electronic communications receive the same Fourth Amendment protections that snail mail and other paper documents receive.

Surveillance

Foreign Intelligence Surveillance Act (FISA) of 1978 and the FISA Amendments Act of 2008: The FISA of 1978 created procedures for physical and electronic surveillance from foreign powers and agents of foreign powers, which may include American citizens and permanent residents suspected of espionage or terrorism. Congress passed an amendment to FISA in 2008 containing Section 702, which authorizes surveillance of people reasonably believed to be located outside the U.S., so long as they are not U.S. citizens or permanent residents.

Communications Assistance for Law Enforcement Act (CALEA): CALEA was enacted in 1994 to enhance the ability of law enforcement agencies to conduct electronic surveillance. It requires that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities and services to have built-in surveillance capabilities.

USA Patriot Act: The Patriot Act was passed in October 2001 in response to the September 11 terrorist attacks. It significantly increased the surveillance and investigative powers of law enforcement agencies. Discussion of specific provisions of the act can be found here.

USA Freedom Act: The USA Freedom Act became law in June 2015, and ended the bulk collection of records about Americans under Section 215 and other provisions of the PATRIOT Act. Rather than bulk collection, specific selection terms are now required, and they must limit the scope of tangible things sought to the greatest extent possible. In addition, the

Act permits companies to make additional reporting ranges to enhance transparency. The Act also requires the Foreign Intelligence Surveillance Court (FISC), which authorizes foreign intelligence surveillance requests, to publish significant opinions.

Additional Technology Issues

Telecommunications Act: President Clinton signed this Act into law in 1996 and it was the first significant overhaul of U.S. telecommunications law since 1934. It required schools, libraries and hospitals to be connected to the Internet by 2000 and required the V-Chip to be installed into every new television, allowing parents to block certain television programs in their homes. The act also limited the number of radio or television stations one entity could own and allowed greater competition between telephone companies.

Computer Fraud and Abuse Act (CFAA): CFAA is the federal anti-hacking law that makes it illegal to intentionally access a computer without authorization or to exceed authorized access. This is primarily a criminal law intended to reduce the instances of malicious hacking, but an amendment to the bill allows for civil actions to be brought under the statute. Some prosecutors have taken advantage of this confusion to bring criminal charges unrelated to hacking. For example, in cases such as *United States v. Drew* and *United States v. Nosal*, the government claimed that violating a private agreement or corporate policy amounts to a CFAA violation.

Digital Millennium Copyright Act (DMCA): Passed in 1998, the Digital Millennium Copyright Act implements two 1996 treaties of the World Intellectual Property Organization (WIPO). It criminalizes technology, devices, or services intended to circumvent controlled access to copyrighted works. In addition, it heightens the penalties for copyright infringement on the Internet.

INNOVATION ECONOMY

Digital Trade: Open Data Flows and Other Key Elements

the DIGITAL 2 DOZEN

The United States is committed to transforming the rules of international trade to promote the free flow of goods, services, and data across a free and open Internet.

1

PROMOTING A FREE & OPEN INTERNET

A free and open Internet enables the creation and growth of new, emerging, and game-changing Internet services that transform the social-networking, information, entertainment, e-commerce, and other services we have today. The Internet should remain free and open for all legitimate commercial purposes. The United States affirms that consumers will be able to access content and applications of their choice when online.

PROHIBITING DIGITAL CUSTOMS DUTIES

The United States recognizes the need for a complete prohibition on customs duties for digital products. This will ensure that customs duties do not impede the flow of music, video, software, and games so our creators, artists, and entrepreneurs get a fair shake.

2

3

SECURING BASIC NON-DISCRIMINATION PRINCIPLES

The United States believes that digital products originating from free trade agreement partner countries cannot be put at a competitive disadvantage in any partner's market. Fundamental non-discrimination principles are at the core of the global trading system for goods and services, and the United States is committed to ensuring that this principle applies to digital products as well.

ENABLING CROSS-BORDER DATA FLOWS

Companies and consumers must be able to move data as they see fit. Many countries have enacted rules that put a chokehold on the free flow of information, which stifles competition and disadvantages American entrepreneurs. The United States seeks to combat these discriminatory and protectionist barriers with specific provisions designed to protect the movement of data, subject to reasonable safeguards like the protection of consumer data when exported.

4

5

PREVENTING LOCALIZATION BARRIERS

Companies and digital entrepreneurs relying on cloud computing and delivering Internet-based products and services should not need to build physical infrastructure and expensive data centers in every country they seek to serve. However, many countries have tried to enforce such requirements which add unnecessary costs and burdens on providers and customers alike. The United States is committed to squarely confronting these localization barriers through specific provisions designed to promote access to networks and efficient data processing.

BARRING FORCED TECHNOLOGY TRANSFERS

Countries should not make market access contingent on forced transfers of technology. The United States will negotiate rules prohibiting countries from requiring companies to transfer their technology, production processes, or other proprietary information to persons in their respective territories.

6

7

PROTECTING CRITICAL SOURCE CODE

U.S. innovators should not have to hand over their source code or proprietary algorithms to their competitors or a regulator that will then pass them along to a State-owned enterprise. The United States will ensure that companies do not have to share source code, trade secrets, or substitute local technology into their products and services in order to access new markets, while preserving the ability of governments to obtain access to source code in order to protect health, safety, or other legitimate regulatory goals.

ENSURING TECHNOLOGY CHOICE

Innovative companies should be able to utilize the technology that works best and suits their needs. For example, mobile phone companies should be able to choose among wireless transmission standards like WiFi and LTE. The United States will negotiate technology choice provisions to ensure that companies are not required to purchase and utilize local technology, instead of technology of their own choosing.

8

9

ADVANCING INNOVATIVE AUTHENTICATION METHODS

The availability of diverse electronic signature and authentication methods protects users and their transactions through mechanisms such as secure online payment systems. The United States will ensure that suppliers can use the methods that they think best for this purpose.

DELIVERING ENFORCEABLE CONSUMER PROTECTIONS

When consumers turn to the Internet for social or commercial purposes, they should be protected. We believe consumer protections, including with respect to privacy, should be embraced by our trading partners. The United States seeks commitments from its free trade agreement partners to adopt and maintain enforceable protections within their markets so that baseline consumer trust is enhanced.

10

11

SAFEGUARDING NETWORK COMPETITION

The United States believes that modern trade agreements must enable our suppliers to build networks in the markets they serve—whether landing submarine cables or expanding data and voice networks—to better access consumers and businesses.

FOSTERING INNOVATIVE ENCRYPTION PRODUCTS

Encryption is increasingly seen as an important tool to address protections of privacy and security in the digital ecosystem. The United States will negotiate rules that protect innovation in encryption products to meet consumer and business demand for product features that protect security and privacy, while allowing law enforcement access to communications consistent with applicable law.

12

13

BUILDING AN ADAPTABLE FRAMEWORK FOR DIGITAL TRADE

New and innovative digital products and services should be protected in trade agreements against future discrimination. By design, U.S. trade agreements will include protections for services and investment that continue to apply as markets change and innovative technologies emerge, unless a specific, negotiated exception applies.

PROMOTING COOPERATION ON CYBERSECURITY

14

The United States will work with its trading partners to share information on threats, as well as help to build cybersecurity capacity to prevent cyber-attacks and stop the diffusion of malware.

15

PRESERVING MARKET-DRIVEN STANDARDIZATION & GLOBAL INTEROPERABILITY

Innovators should not have to design products differently for each market they seek to serve—that is why we have the global standards process, where industry leads and the best technologies win. The United States will ensure that countries cannot arbitrarily demand that less competitive national standards be forced into innovative American products.

ELIMINATING TARIFFS ON ALL MANUFACTURED PRODUCTS

16

The United States will agree to eliminate tariffs on all product exports manufactured in the territory of its free trade agreement partners, including information and communication technology (ICT) products. In addition, the United States will ask its free trade agreement partners to commit to work to join the WTO Information Technology Agreement (ITA), which will eliminate tariffs on a broad range of information technology products, including countries that have not previously joined the ITA.

17

SECURING ROBUST MARKET ACCESS COMMITMENTS ON INVESTMENT & CROSS-BORDER SERVICES, INCLUDING THOSE DELIVERED DIGITALLY

The United States will seek and maintain strong investment and cross-border services commitments. In particular, the United States will seek to provide U.S. digital service providers with the certainty of knowing that the services they provide—including both technology-related support services such as cloud computing and services like consulting, marketing, and advertising more generally—can be legally offered in the countries of its free trade agreement partners.

ENSURING FASTER, MORE TRANSPARENT CUSTOMS PROCEDURES

18

The United States will seek to include in its trade agreements strong commitments on customs procedures and trade facilitation (including express shipments) to ensure that border processing will be quick, transparent, and predictable. These kind of administrative barriers can often be a bigger problem than tariffs for U.S. exporters of digital equipment. The United States also will seek to facilitate paperless trading through the use of electronic customs forms.

19

PROMOTING TRANSPARENCY & STAKEHOLDER PARTICIPATION IN THE DEVELOPMENT OF REGULATIONS & STANDARDS

The development of new regulations and standards can pose a significant challenge to ICT suppliers, whose product cycles are short and whose regulatory environment is constantly evolving. United States trade agreements will contain strong commitments on transparency, stakeholder participation, coordination, and impact assessment for new regulatory measures, standards, and conformity assessment procedures. The United States will also seek to negotiate chapters on regulatory coherence to further minimize such non-tariff barriers to trade.

ENSURING FAIR COMPETITION WITH STATE-OWNED ENTERPRISES

The United States will seek to conclude robust commitments to ensure that State-owned enterprises competing with U.S. exporters, including in the ICT sector, compete on the basis of quality and price rather than on the basis of discriminatory regulation, subsidies, or favoritism.

20

21

PROMOTING STRONG & BALANCED COPYRIGHT PROTECTIONS & ENFORCEMENT

Copyright protections are essential to ensuring that the coders, designers, and product managers behind a product have the freedom to create and are compensated for their creative works—just like musicians and authors. The United States seeks the strong copyright protection and enforcement provisions that we have in U.S. law, and the commitment of our free trade agreement partners to continuously seek to achieve an appropriate balance in their copyright systems, including through copyright exceptions and limitations. The United States also seeks copyright safe harbors for legitimate Internet Service Providers (ISPs) comparable to those in U.S. law.

ADVANCING MODERN PATENT PROTECTION

The United States will reinforce the global standard of transparent, strong, and balanced patent protections for cutting edge innovation, including appropriate limitations and exceptions drawn from international commitments. These provisions protect the jobs and innovative solutions generated by U.S. entrepreneurs in areas ranging from solar panels to smart manufacturing.

22

23

COMBATTING TRADE SECRET THEFT

The United States will negotiate provisions to address the problem of corporate espionage, including trade secret theft conducted by State-owned enterprises. The United States will ask its free trade agreement partners to establish criminal procedures and penalties for trade secret theft, including by means of cyber theft, while preserving domestic laws that protect whistleblowing.

RECOGNIZING CONFORMITY ASSESSMENT PROCEDURES

Conformity assessment procedures verify that products, including ICT products, meet required standards and technical regulations, but overly burdensome conformity assessment procedures in foreign countries can hinder ICT exports. The United States will require its free trade agreement partners to provide "national treatment" to one another's conformity assessment bodies, so testing and certification performed by a qualified conformity assessment body will be accepted as consistent with another partner's requirements.

24

Computer & Communications Industry Association
Tech Advocacy Since 1972

CCIA Summary of USTR's 2017 NTE Report: Focus on Digital Trade

In 2017, the United States Trade Representative (USTR)'s National Trade Estimate (NTE) report on trade barriers separately highlighted for the first time a number of barriers specific to *digital* trade, which could undermine the United States' global leadership in the digital economy. USTR cited ongoing and emerging barriers such as "restrictions or other discriminatory practices affecting cross-border data flows, digital products, Internet-enabled services, and other restrictive technology requirements." *Selected examples of the digital trade barriers highlighted by USTR are excerpted below.*

Data and Infrastructure Localization: Various countries have implemented data localization policies such as mandated server localization or local storage of domestic citizens' data. While such policies are ostensibly aimed at ensuring domestic privacy or promoting local economic development, studies have cast doubt on the effectiveness of these policies to achieve either goal.

China - "A number of elements of China's new Cybersecurity Law, issued in November 2016, authorize Chinese agencies to further restrict market access for cloud computing and other Internet-enabled related services, based on data and facilities localization policies applicable to services deemed critical."

European Union - "[Last year], the United States and the EU concluded the EU-U.S. Privacy Shield Framework to provide U.S.-based organizations a mechanism to comply with EU data protection requirements when transferring personal data from the EU to the United States in support of transatlantic commerce." [. . .] "The Privacy Shield Framework supports cross-border trade estimated to be in the hundreds of billions of dollars." [. . .] "As of the end of 2016, two legal challenges had been filed against the Privacy Shield in the EU's General Court (lower court). . . . Finally, the Privacy Shield Framework also provides for an annual Commission review of its effectiveness."

Russia - "In 2015, Russia adopted legislation requiring that certain data collected electronically by companies on Russian citizens be processed and stored in Russia." [. . .] "The 2015 law not only implicates the provision of cross border services, but it also restricts a company's options with regard to the location of its servers for storing the data. . . . In November 2016 . . . [Roskomnadzor] blocked access in Russia to a U.S.-based business networking service site based on a finding of non-compliance, despite the fact that the company had no physical presence in Russia."

South Korea - "The 2011 Personal Information Protection Act . . . requires data exporters to provide customers with extensive information about the data transfer, including the destination of the data, any third party's planned use for the data, and the duration of retention. These restrictions . . . effectively privilege Korean third-party services over foreign services." [. . .] "In April 2016, Korea amended its IT Network Use and Protection Act, which . . . impose[s] significant penalties for violating data protection standards,

including heavy fines for telecommunications and online service providers that transfer personal data cross-border without consent."

Filtering and Blocking: Perhaps the most apparent barriers to digital trade are the outright filtering and blocking of U.S. Internet platforms and online content, with one study finding that countries lose $23.6 million (per 10 million in population) for every day that the Internet is shut down. Notwithstanding these costs, governments continue to filter and block Internet content, platforms, and services for various reasons.

China - "China continues to engage in extensive blocking of legitimate websites, imposing significant costs on both suppliers and users of web-based services and products. According to the latest data, China currently blocks 11 of the top 25 global sites, and U.S. industry research has calculated that up to 3,000 sites in total are blocked, affecting billions of dollars in business, including communications, networking, news and other sites."

Legal Liability for Online Intermediaries: Foreign countries have frequently imposed substantial penalties on U.S. Internet companies for conduct of third parties—something that is not permitted under U.S. law and that impedes the ability of U.S. online platforms to deliver services abroad. This not only hurts Internet companies, but also denies local small and medium-sized enterprises Internet-enabled access to the global marketplace, similarly discouraging investment in and growth of domestic startups.

Brazil - Legislative proposals that would modify Brazil's 2014 Civil Rights Framework for the Internet, or Marco Civil, include "a provision that would force online companies to assume liability for all user communications and publications . . . " Another proposal would "amend Marco Civil to allow the judiciary, in consideration of public interest, proportionality, scope, and speed, to block Internet sites and applications to deter to cybercrime."

European Union - The new General Data Protection Regulation (GDPR) is "more complex than its predecessor and includes several elements with a potentially significant impact on the interests of U.S. companies . . . , " including "joint liability obligations, a data protection officer requirement, data portability, data breach notification, parental consent requirements, and the "right to be forgotten."" [. . .] "The GDPR codifies the 2014 decision of the CJEU that imposed a right for EU citizens to demand that search engines remove information that is inaccurate, inadequate, irrelevant, or excessive for the purposes of data processing." The "right to be forgotten" has the "potential to conflict with free speech and to restrict access to information of legitimate public interest."

India - "India's 2011 Information Technology Rules fail to provide a robust safe harbor framework to shield online intermediaries from liability for third-party user content. Any citizen can complain that certain content is "disparaging" or "harmful," and intermediaries must respond by removing that content within 36 hours. Failure to act, even in the absence of a court order, can lead to liability for the intermediary."

Imbalanced Copyright: Balanced copyright rules such as fair use and related limitations and exceptions have been critical to the growth of the U.S. technology and Internet economy. Within the last thirty years, such rules have enabled the development of innovative new products and services such as the VCR, DVR, iPod, cloud

computing, search engines, social media services, and 3D printing—innovations that are jeopardized by weak or nonexistent limitations and exceptions in the copyright laws of other countries.

> *European Union* - "Over the past several years, certain EU Member States have adopted measures requiring fees associated with online news aggregation services. Specifically, the measures require news aggregators, which provide "snippets" of text from other news sources, to remunerate those other sources. One Member State has also introduced a similar measure with respect to digital images. These measures are intended to address publishers' and visual artists' challenges in adapting to the digital marketplace, but measures that disproportionately affect only one group of foreign-based service suppliers in the digital ecosystem may exacerbate those challenges to the detriment of all participants in the marketplace."

Technology Requirements: Onerous technology requirements specific to particular countries restrict digital trade for ostensibly legitimate national security or public policy objectives, but often amount to protectionist measures that are vaguely construed, inadequately articulated, and thus nearly impossible to satisfy—chilling innovation and investment in digital platforms and their beneficiaries.

> *Brazil* - "Presidential Decree 8135/2013 requires that government agencies procure email, file sharing, teleconferencing and Voice over Internet Protocol (VoIP) services from a federal Brazilian public entity such as the SERPRO, Brazil's Federal Data Processing Agency. Subsequent implementing regulations . . . impose additional requirements including auditing of government contractors' systems and access to their source code."

> *China* - "Onerous requirements on the use of encryption, including intrusive approval processes and, in many cases, mandatory use of indigenous encryption algorithms (e.g., for WiFi and 4G cellular products), continue to be cited by stakeholders as a significant trade barrier. The United States will continue to monitor implementation of existing rules, and will remain vigilant toward the introduction of any new requirements hindering technologically neutral use of robust, internationally standardized encryption."

> *Russia* - "[T]he Yarovaya Amendments, under the guise of fighting terrorism, may require companies to assist government authorities in decrypting user communications and prohibits encryption measures unless a decryption key is provided to the Russian authorities upon request."

Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information

Summary

The transformative economic benefits of the Internet are under threat, as increasing numbers of governments move to impose onerous limits on information flow. The international community must take action to ensure the free flow of information online. Governments should honor existing international obligations including under the World Trade Organization (WTO) Agreement, prevent trade barriers created by information regulation, and develop new international rules that provide enhanced protection against these trade barriers of the 21st century.

To realize the full potential of the Internet as a global marketplace and platform for innovation, policymakers in the United States, the European Union, and elsewhere should pursue three steps to break down barriers to free trade and Internet commerce:

- Focus on and publicly highlight as unfair trade barriers those practices by governments that restrict or disrupt the flow of online information services.
- Take appropriate action where government restrictions on the free flow of online information violate international trade rules.
- Establish new international trade rules under bilateral, regional, and multilateral agreements that provide further assurances in favor of the free flow of information on the Internet.

This is an ambitious but achievable agenda. It offers opportunities for the U.S. government to better align the nation's trade priorities with the global economy and, in turn, create new jobs and export opportunities for the U.S. It can also provide concrete incentives for other governments to reduce or stop the restriction and disruption of information on the Internet.

Context

The need to protect the free flow of information online is more clear than ever. A confluence of trends has created a new international trade and business environment that calls for governments to ensure that the Internet remains open for global business.

The Internet has transformed traditional commerce, creating an astounding array of new economic opportunities and expanding international trade. More than three million Americans now owe their jobs to the Internet, and hundreds of thousands of businesses use the Internet to reach once-inaccessible international markets. This has had significant ripple effects throughout national and local economies, helping drive economic and job growth in the information age.

An open Internet has been and remains an absolutely critical component of the new information economy's ability to empower individuals and create shared information markets. Closed systems are antithetical to the Internet's success and will significantly disable its potential to support trade and innovation going forward.

But governments around the world are restricting, censoring, and disrupting the free flow of online information in record numbers. More than 40 governments now engage in broad-scale restriction of online information, a tenfold increase from just a decade ago. Today more governments are incorporating surveillance tools into their Internet infrastructure; blocking online services in their entirety; imposing new, secretive regulations; and requiring onerous licensing regimes that often discriminate against foreign companies. These actions unnecessarily restrict trade, and left unchecked, they will almost certainly get worse.

Taken together, these actions have created a very difficult international trade environment in which information platforms and services are impeded, businesses' revenue streams are undercut, access to information in key markets is disrupted, and discrimination against U.S. and other multinational businesses grows. Every day, evidence accumulates that governments must take concerted action to protect and promote the free flow of online information and Internet trade.

Section I of this paper demonstrates how the Internet has changed the global economy and had a positive impact on international trade. Section II describes both the range and common characteristics of government regulations and restrictions on information flow. Section III outlines the trade effects of these practices and describes the harm to economic and trade interests. Section IV and the technical appendix analyze how current trade rules can and should be used to contest

trade-restrictive Internet barriers related to information flow. Section V lays out a negotiating agenda for the future and makes recommendations about new trade rules needed to address these barriers.

I. The Internet's impact on economic growth and trade

The past decade has clearly demonstrated the Internet's vital and ever-increasing role in generating global economic growth and international trade, and economists and technologists today regularly refer to the "Internet economy." The Internet has rightfully been labeled a "general purpose technology enabler" – a once-in-a-generation technological development that fundamentally changes how economic activity is organized and enables a productivity leap. It has "enable[d] the emergence of new business models, new processes, new inventions, new and improved goods and services and … increase[d] competitiveness and flexibility in the economy, for example by the increased diffusion of information at lower cost." According to the Organization for Economic Cooperation and Development, the Internet's impact on productivity may exceed the effect of any other technology enabler to date, including electricity and the combustion engine.[1]

The tremendous spread of the Internet – faster than the spread of any previous technology – has also created new, rapidly expanding markets. Online traffic has increased at a compound annual growth rate of 66 percent over the past five years.[2] Today more than one-quarter of the world's population (1.7 billion people) uses this technology to communicate, inform, create, and buy and sell across borders.[3] These 1.7 billion Internet users are a massive new consumer base for both Internet services like email and the hard goods and services that are increasingly advertised, marketed, or sold online.

Internet intermediaries, the "platform" companies that provide such services as search, commerce sites, and applications, represent a substantial and growing segment of developed economies. These businesses generally act as intermediaries between "upstream" services or goods being supplied, and users: e-commerce markets like eBay and Amazon that bring buyers and sellers together; search engines like Google and Bing that help users find resources on the web; "app stores" that allow computer programmers to sell their software products for particular devices; video or photo sharing sites like YouTube and Flickr where user-generated content is posted; social services like Twitter and Facebook that promote connections among Internet users; and many, many others -- including some that are likely to start up in a garage somewhere in the United States in the future.

These companies are major sources of employment and drivers of economic growth. In the United States, the Internet ad-supported industry has created more than 3 million jobs.[4] These firms range from familiar multinational companies to some 20,000 small businesses with fewer than 500 employees.[5] These industries contribute at least $300 billion to the U.S. GDP.[6] Annual Internet-

---

[1] Org. for Econ. Cooperation & Dev. [OECD], *Broadband and the Economy: Ministerial Background Report* 8-9, OECD Doc. DSTI/ICCP/IE(2007)3/FINAL (May 2007).

[2] Fed. Commc'ns Comm'n [FCC], *Connecting America: The National Broadband Plan* ch. 4 (2010).

[3] Miniwatts, Internet World Stats, *Internet World Users by Language: Top Ten Languages* (chart) (Sept. 30, 2009), http://www.internetworldstats.com/stats7.htm; Int'l Telecomm. Union [ITU], *The World in 2009: ICT Facts and Figures* 1 (2009), http://www.itu.int/ITU-D/ict/material/Telecom09_flyer.pdf. The total number of fixed broadband subscribers reached nearly 500 million by the end of 2009. *Id.* at 5.

[4]This figure does not include aspects of the Internet economy that are not ad-supported, so the number including those benefiting from this economy is much higher. Hamilton Consultants, *Economic Value of the Advertising Supported Internet Ecosystem* 24 (June 10, 2009).

[5] Hamilton Consultants, *Economic Value of the Advertising Supported Internet Ecosystem* 56 (June 10, 2009).

based commerce worldwide is expected to soon reach $1 trillion.[7] In the United States alone, online retail sales were over $132 billion in 2008.[8] Globally, Internet and telecom services contributed 3.3 percent of GDP in 2004, compared with 1.8 percent in 1990, with virtually every single economy enjoying growth in the sector.[9]

Given the borderless nature of the Internet, it should surprise no one that Internet firms have become important exporters in their own rights, as well as key generators of international trade. According to a study by Hamilton Consultants, large U.S. Internet corporations earn about one-half their revenues outside the United States.[10] In the case of Google, revenues from outside of the United States comprised 53 percent of total revenues in the first quarter of 2010, and more than half of Google searches come from outside the United States.[11]

Even in more traditional trade sectors, like the goods and services businesses, the Internet has also been transformative. The Internet has empowered businesses of all sizes to reach international markets in ways unimaginable a generation ago. It has dramatically reduced the high entry costs to export markets that has for centuries kept most small business limited to local geography. This transformation of industry happens in both the industrial and developing world. In the U.S. state of Georgia, a small manufacturing operation is reaching out to international customers through Internet advertising.[12] In Idaho, a wilderness tourism company has attracted international customers through online search ads.[13] And in the South American nation of Guyana, women are using online marketing to sell hand-woven hammocks to people around the world.[14]

Many companies rely on the Internet, including particular websites, as their key advertising platform. For instance, companies are projected to spend over $225 billion on Internet advertising over the next three years (2011-2013).[15] Google alone generated more than $54 billion in economic activity in the United States in 2009 based largely on returns that businesses received from advertisements run next to search results and on websites.[16]

---

[6] Hamilton Consultants, *Economic Value of the Advertising Supported Internet Ecosystem* 4 (June 10, 2009).
[7] Brian Hindley & Hosuk Lee-Makiyama, *Protectionism Online: Internet Censorship and International Trade Law* 3 (ECIPE, Working Paper No. 12/2009), *available at* http://ecipe.org/publications/ecipe-working-papers/protectionism-online-internet-censorship-and-international-trade-law.
[8] U.S. Census Bureau, *Estimated Quarterly U.S. Retail Sales (Adjusted): Total and E-commerce* (chart) (May 15, 2009), http://www.census.gov/mrts/www/data/html/09Q1table3.html.
[9] Int'l Telecomm. Union [ITU], *digital.life: ITU Internet Report 2006* 73 (2006), http://www.itu.int/osg/spu/publications/digitalife/docs/digital-life-web.pdf.
[10] Hamilton Consultants, *Economic Value of the Advertising Supported Internet Ecosystem* 7 (June 10, 2009). Note that the jobs measured by Hamilton Consultants are merely advertising supported jobs. As such, the number of jobs created by the broader advertising industry is higher.
[11] Google Investor Relations, *Google Announces First Quarter 2010 Financial Results* (Apr. 15, 2010), http://investor.google.com/earnings/2010/Q1_google_earnings.html.
[12] Google, *Google in Georgia*, in *Google's Economic Impact: United States 2009* (2009), *available at* http://www.google.com/economicimpact/pdf/google_economicimpact.pdf.
[13] Google, *Google in Idaho*, in *Google's Economic Impact: United States 2009* (2009), *available at* http://www.google.com/economicimpact/pdf/google_economicimpact.pdf.
[14] Simon Romero, *Weavers Go Dot-Com, and Elders Move In*, N.Y. Times, Mar. 28, 2000, *available at* http://www.nytimes.com/learning/teachers/featured_articles/20000330thursday.html.
[15] PriceWaterhouseCoopers, *Global Entertainment and Media Outlook 2009-2013* 30 (2009).
[16] Google, *Google's Economic Impact: United States 2009* (2009), *available at* http://www.google.com/economicimpact/pdf/google_economicimpact.pdf.

The Internet's impact on export growth is clear and demonstrable. According to one recent study, a 10 percent increase in a country's overall Internet penetration is associated with a 1.7 percent increase in export growth in the services sector. A lower, but similar correlation pertains to trade in goods.[17]

As a new dynamic and open force in the global economy, the Internet has helped produce phenomenal change and growth. This growth has been accompanied by increasing demand worldwide for information and services from beyond national borders. While many governments have welcomed the new trade, some have recoiled at the new openness – and are determined to restrict the flow of information across the Internet.

II. Government disruption of the free flow of information on the Internet

In the early years of the Internet, it was widely believed that government attempts to censor online communication would inevitably fail. President Clinton spoke of efforts by governments to block the Internet being like trying to nail Jell-O to the wall. Internet technologist John Gilmore observed that, "The Net interprets censorship as damage and routes around it."[18] But as time went on – and governments proved the optimists wrong – that utopianism subsided, replaced by a more realistic understanding of the promise and perils of the technology.

In less than a decade, as noted above, more than 40 governments have instituted broad-scale restrictions of information flow on the Internet. They have become both increasingly sophisticated and successful in controlling many aspects of the Internet and restricting information to varying degrees. They have moved from a more simplistic approach of denying access to more subtle techniques of controlling access, techniques that can be even more damaging than denial of access in the long run.[19]

Governments have pursued four basic strategies to controlling information on the Internet:

- Technical blocking of access to an entire Internet service (*e.g.*, a search engine, an online store, a platform for hosted content) or specific keywords, web pages, and domains.
- Licensing requirements or other means to force companies to remove search results, making it more difficult for users to locate particular content.
- Take-down requirements demanding the removal of certain websites, enforced by legal orders or by making whole domains invisible to users.
- Encouragement of self-censorship through means including surveillance and monitoring, threats of legal action and informal methods of intimidation.[20]

---

[17] Caroline Freund & Diana Weinhold, *The Internet and International Trade in Services*, 92 A.E.A. Papers & Proc. 236, 236 (2002); *see also* Caroline Freund & Diana Weinhold, *The Effect of the Internet on International Trade*, 62 J. Int'l Econ. 171, 172 (2004) (for trade in goods).

[18] Jack L. Goldsmith & Tim Wu, *Who Controls The Internet? Illusions of a Borderless World* 90 (2006).

[19] Ronald Deibert & Rafal Rohozinski, *Beyond Denial: Introducing Next-Generation Information Access Controls*, in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* 4-7 (Ronald Deibert et al. eds., 2010).

[20] These four basic techniques were identified by the Open Net Initiative, a collaborative partnership of researchers at the University of Toronto, Harvard University, the University of Cambridge and Oxford University. See Open Net Initiative, *About Filtering*, http://opennet.net/about-filtering. Others use different taxonomies to describe the range of efforts to control information on the Internet. *See, e.g.*, Congressional-Executive Commission on China, *Hearing on Google and Internet Control in China: A Nexus Between Human Rights and Trade?* (Mar. 24, 2010) (statement of Rebecca MacKinnon, Visiting Fellow, Center for Information Technology Policy, Princeton University).

Most government control of Internet information consists of either direct government blockage of an Internet service, or regulation of the content they may carry. Direct government blockage of an Internet service is tantamount to a customs official stopping all goods from a particular company at the border. In other cases, governments demand that as a condition of providing service to a particular market, companies like Internet service providers and search engines block or disrupt services, websites, and content. In either situation, the result is a restriction on the ability of Internet companies to provide their services (and generate revenue accordingly), and a disruption in the trade of all other enterprises that use these services.

Some common characteristics of government restriction of the Internet include the following:

Opaque regulations that disrupt information flow

Governments in some countries impose requirements on online service providers without making these rules publicly available or establishing a legal process. Governments may make demands orally, threaten to revoke licenses or take other punitive action when informal orders are not heeded.

Some countries explicitly make it a crime for a service provider to reveal requests made by government authorities – even where there is no law enforcement or similar rationale for secrecy.

As two leading Harvard Internet scholars have concluded, "With the exception of a few places, no state seems to communicate much at all with the public about its process for blocking and unblocking content on the Internet."[21] The lack of transparency also enables governments to engage in other excesses as part of efforts to limit information. And it denies exporters an opportunity to seek redress, or even a way to discover what is being done to limit their access to this market.

Wholesale blocking of services

Governments or legal bodies regularly block in their entirety a range of information services including video sites, social networks and blogging platforms.

Turkey is a recent case in point. An individual public prosecutor in Ankara was able to block YouTube access for all Turkish users for over two years after YouTube rejected his demand that they remove a number of videos from the site globally because they were deemed to be breaching a Turkish law that protects the reputation of its founder Kemal Ataturk. An offer to restrict viewing for objectionable videos within Turkey was deemed inadequate by the Prosecutor - only the worldwide application of the Turkish law would have seen the ban reversed. Recently the videos at the heart of the ban were automatically removed as the result of a copyright claim. These were reinstated (though restricted based on IP address for Turkey) when the claim was not upheld. As a result, YouTube is newly accessible from Turkey but the power to ban it again in the same way remains until the law is clarified.

This service blocking is by no means limited to video platforms, but extends to all services that enable free flow of information to users in countries restricting this information. China

[21] Jonathan Zittrain & John Palfrey, *Internet Filtering: The Politics and Mechanics of Control*, in *Access Denied: The Practice and Policy of Global Internet Filtering* 36 (Ronald Deibert et al. eds., 2008).

has shut off Facebook, Flickr, and Twitter many times. Foursquare, one of the newest social networking services that has recently risen in popularity, was blocked in advance of June 4, 2010, in response to the number of users who set their location to Tiananmen Square as a way of paying their respects online.

The effect of such actions on trade and communications is often drastic, because it is usually the services most used by local users that are blocked by governments. Livejournal, a popular blogging service in many parts of Eastern Europe, has been intermittently blocked by the governments of Turkmenistan, Uzbezikstan, and Kazakhstan over the past two years. Another blogging service, WordPress, was blocked by Guatemala during a political crisis in June 2009. In the aftermath of the disputed Iranian elections, when citizens began sending out material unfavorable to the ruling regime, that government blocked Twitter, YouTube and Google's email service, Gmail. Google's blogging service has been blocked in multiple countries, as has its social networking site, Orkut.

Vietnam has blocked Facebook since last year, and is threatening to filter more sites in Internet cafes in Hanoi with a new regulation, to be fully effective in 2011. And Pakistan, Turkey, and Afghanistan have recently released court orders that allow the government to monitor and block sites like Google, Yahoo!, Amazon, MSN, Hotmail, and Bing for content considered "blasphemous" or anti-Islamic.

Bias against foreign competitors

In October 2007, Chinese officials – angry over the U.S. Congress award of its Gold Medal to the Dalai Lama and the opening of a YouTube domain in Taiwan – manipulated the so-called Great Firewall so that users who typed in web addresses for the three major U.S.-based Internet search engines (run by Google, Microsoft, and Yahoo!) were taken not to their site of choice but rather to the Chinese-owned search engine, Baidu.

Governments including China and Vietnam censor both services and content at international telecommunications network gateways, and subject Internet traffic coming from outside the country to special filtering regimes. This can result in degradation of services that do not originate within the country as authorities pick and choose what information foreign entities will be allowed to provide.

Arbitrary and capricious behavior

To make matters worse, governments sometimes apply laws and regulations haphazardly or maliciously. Officials in a number of countries have blocked or disrupted services because particular content offended their personal sensibilities or exposed personal improprieties, even when the content had no plausible connection to the government's objectives, or was available through other services as well. In other cases, there has been direct government intervention that has hurt both the reputation and sales of Internet firms.

In June 2009, government-controlled media in China singled out Google as a purveyor of pornography in order to justify the order that computer manufacturers install the so-called "Green Dam" software, technology that would allow the government to block users from

seeing "harmful content." Although many Chinese-owned services and portals also carry pornography, the Chinese government shone its spotlight only on Google sites.[22]

The examples and anecdotes cited above are part of a larger trend that worries experts at the Open Net Initiative, Freedom House, Reporters Without Borders and other groups that track disruptions of online information flows. There is a growing consensus that governments must do more than appeal for the protection of human rights and encourage development of tools that allow users to bypass government firewalls. Censorship on the Internet poses a significant economic threat to companies seeking a level playing field as they establish markets overseas.

III. The impact of government restrictions on information in trade

Limitations on the free flow of information and restrictive Internet regulations are a clear threat to open markets and trade. Governments that limit or block the flow of information threaten not only the ability of companies to access and compete in their markets, but also threaten the very traits of the Internet that have made it into an engine of economic growth and put at risk the ability of the Internet-related business to continue expanding their exports, employment, and innovation.

Block the "ports" of 21st century trade

Internet filtering makes it harder for Internet companies to reach their customers, and it means that the businesses that rely on the Internet are likely to experience lower productivity.[23] According to an Australian government-commissioned study, experimental Internet filtering at the ISP level degraded network performance by between 2 percent and 87 percent, depending on the filtering software.[24] And when such filtering is applied only to foreign traffic, it means that foreign websites, and those businesses that rely on foreign websites to market and sell their products, become a second-best option to their local competitors.

The Internet is a 21st century trading route, and so when it is impeded, the commerce that passes through it is impeded too. A study that compared the role of the Internet and that of port facilities in trade facilitation, and found that the Internet is at least as important in facilitating trade: Improving the speed and affordability of Internet access could lead to a 4 percent increase in trade in manufactured goods, compared to a 2.8 percent increase associated with improving port efficiency.[25]

Hurt companies seeking to export their services to new markets

---

[22] Simon Elegant, *Chinese Government Attacks Google Over Internet Porn*, Time, June 22, 2009, *available at* http://www.time.com/time/world/article/0,8599,1906133,00.html; Wang Xing & Cui Xiaohuo, *Google "Used" in Online Porn Tiff*, China Daily, June 22, 2009, *available at* http://www.chinadaily.com.cn/china/2009-06/22/content_8306840.htm.

[23] Duncan Riley, *The Economic Cost of Internet Censorship in Australia*, Inquisitr, Feb. 5, 2009, *available at* http://www.inquisitr.com/17448/the-economic-cost-of-internet-censorship-in-australia.

[24] Australian Commc'ns & Media Auth., *Closed Environment Testing of ISP-Level Internet Content Filtering* 48 (2008). While the study predicted that "moderate to nearly nil performance degradation is possible," *id.* at 52, actual degradation depends on the technology used, and the study demonstrated substantial variance in the performance of different filters.

[25] United Nations Economic and Social Commission for Asia and the Pacific & Asian Development Bank, *Designing and Implementing Trade Facilitation in Asia and the Pacific* 85 (2009), *available at* http://www.unescap.org/publications/detail.asp?id=1352 (citing John S. Wilson et al., *Assessing the Potential Benefit of Trade Facilitation: A Global Perspective* 24-32 (World Bank, Policy Research Working Paper 3224, 2004)).

When a foreign government blocks or technically interferes with a website, it has either barred or undercut that business' access to the market. The Internet business cannot reliably offer its services, attract users to its site, or serve advertisements to Internet users in that country. The government action is the equivalent of shuttering the windows of a brick-and-mortar store, or, in the case of technical interference, stopping every third or fourth customer from entering the store. And the problems are particularly pronounced where a government interferes with a so-called Internet intermediary website, as it affects all of the business and individuals that use the site to communicate, trade, and advertise.

Consider the example where a government takes a website out of service for one week. For the intermediary company offering the service, that break will decrease revenue for the site by at least 2 percent on an annual basis.[26] For the company that uses the platform to advertise or sell goods and services, there will be a similar drop and a loss of trust in the platform. And given users' tendency to move to new services when the ones they use do not load quickly, let alone services that disappear for a week – the resulting perception of unreliability could result in both short- and long-term decreases in traffic.[27] In one study, over three-quarters of consumers said they would be less likely to return to a site that took too long to load.[28]

Beyond the impairment of speed and availability of sites, restrictive rules around the flow of information change the nature of the service that an Internet company can provide. The core business of intermediary companies is to provide access to the search results, hyper-links, websites, emails, blog entries, news, maps, calendars, spreadsheets, photos, and videos that drive interactions across the Internet; they are providing information and communication platforms. The utility of those services and the trust of users are both compromised when the product contains incomplete and distorted information.

Provide unfair advantage to local companies

When governments choose to manipulate the market in favor of local firms, it is naturally harder for foreign firms to compete. In China, for instance, numerous U.S. Internet services have been kept out or severely restricted, while Chinese versions of the same services have been permitted to operate; and in some cases, the Chinese sites contain their own share of "offensive" content. As an article in *Foreign Policy* noted:

> [I]n July 2009, after the riots...in Xinjiang, China blocked Facebook. Meanwhile direct Chinese copies of Facebook, Ren Ren Wang and Kai Xin Wang, have been enjoying enormous success. Also in the aftermath of the Xinjiang riots, microblogging site Twitter was cut off by the Chinese firewall for similarly dubious reasons. Less than two months later, Chinese Internet giant Sina launched a near identical microblogging service. ... Even a seemingly harmless site, like [Flickr], has been blocked in China, while its identical clone Bababian has grown steadily with foreign technology and no competition. Likewise, blog-hosting sites Blogger and WordPress have long been blocked in China. Instead Chinese

---

[26] Brian Hindley & Hosuk Lee-Makiyama, *Protectionism Online: Internet Censorship and International Trade Law* 6 (ECIPE, Working Paper No. 12/2009), *available at* http://ecipe.org/publications/ecipe-working-papers/protectionism-online-internet-censorship-and-international-trade-law.

[27] ShanShan Qi et al., *A Study of Information Richness and Downloading Time for Hotel Websites in Hong Kong*, in *Information and Communication Technologies in Tourism: 2008* 267, 268 (Peter O'Connor et al. eds. 2008) (citing C. Ranganathan & S. Ganaphy, *Key Dimensions of Business-to-Consumer Websites*, Info. & Mgmt., 39(6), 457-465 (2002)),

[28] JupiterResearch, *Retail Web Site Performance: Consumer Reaction to a Poor Online Shopping Experience* 5-7 (2006), *available at* http://www.akamai.com/dl/reports/Site_Abandonment_Final_Report.pdf.

> netizens use Tianya, the 13th-most popular site in China. Far from being a sanitized land of boring blogs about daily activities ... [it] is a vitriolic, sensationalized, and hate-filled arena that makes Western gossip sites seem like the *Economist*.

Impede business operations

When governments impose non-transparent and arbitrary regulation on online services – as is often the case under restrictive information regimes – they make it difficult for businesses to execute commercial plans. To successfully export to or invest in a new market, a company needs to be able to understand the rules of the road and have some level of confidence that the government will not arbitrarily interfere with its business.

Hurt businesses that rely on the Internet to advertise or sell goods and services

Companies that sell or advertise goods and services on intermediary sites are severely impacted when the site is blocked or becomes unstable in a particular country: the small business that advertises on Google search through AdWords but does not reach certain markets because the search service is blocked; the artist and music publisher who do not reach a certain market because an entire online music store is blocked; the manufacturer selling its goods on an online marketplace like eBay that is blocked.

These restrictions on trade inordinately impact small businesses that only have the Internet as a means to reach a broad audience. For companies that are breaking into new markets, disruption of the services for even short periods of time can disrupt business plans and block their visibility to new customers at critical moments.

Hurt downstream businesses that cannot access services or goods

Businesses and consumers that rely on access to the Internet services are adversely impacted when these services are blocked or impeded as a result of Internet censorship. To take one example, the recent blockage of Google Docs in Turkey caused substantial disruptions for businesses that rely on that Internet service. Said one Turkish service provider: "We have created a Google document [page] and were running our operations from there; now we cannot communicate." As a result, they will be forced to migrate to more expensive platforms or applications that are not hampered by government restrictions.

Put the global Internet at risk

Restrictive Internet regulations have a broader negative effect on the shape and architecture of the Internet. The Internet was developed as an open network of networks: "The decision to make the Web an open system was necessary in order for it to be universal. You can't propose that something be a universal space and at the same time keep control of it."[29] This remains true today.

Governments that build censorship into networks change the architecture and nature of the Internet in ways that damage trade and innovation. As the Federal Communications Commission recently observed, "Today's Internet embodies a legacy of openness and transparency that has been critical

[29] World Wide Web Consortium (W3C), *Frequently Asked Questions*, http://www.w3.org/People/Berners-Lee/FAQ.html (quoting Sir Tim Berners-Lee, an engineer widely credited with creating the concept and protocols of the World Wide Web).

to the network's success as an engine for creativity, innovation, and economic growth;"[30] "[i]ts continued health and growth...depend on its continued openness."[31] This statement is true not only in the United States, but worldwide; any restrictions on the flow of information globally affect the Internet here.

Fragmenting the global Internet into "local" networks operating under different rules necessarily complicates and slows trade and economic growth. It makes information delivery uneven and re-creates the disparities among people's access to information that the Internet has heretofore succeeded in eliminating. A divided Internet impedes the ability of businesses to reach a global market and impedes the collaboration and network effects that create so much of the value for many Internet businesses and Internet users.

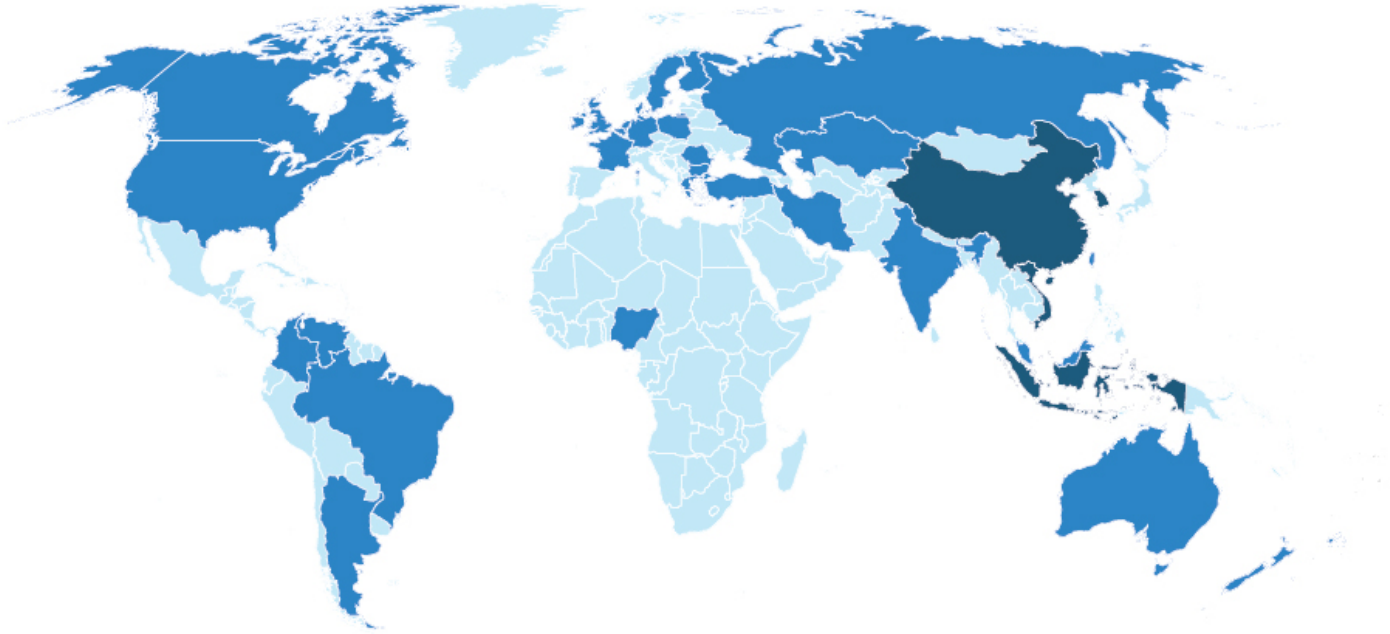
In sum, when Internet services are blocked or restricted, or the Internet is regulated in a non-transparent or arbitrary manner, the substantial economic and trade benefits of the Internet are put at risk. Trade officials and policymakers should be deeply concerned about the impact of Internet information restrictions on economic growth and trade interests. And, they should be ready to use current trade rules and negotiating forums to reduce this threat.

[30] Fed. Commc'ns Comm'n [FCC], Notice of Proposed Rulemaking, *In the Matter of Preserving the Open Internet,* ¶ 17, FCC 09-93 (Oct. 22, 2009).

[31] Fed. Commc'ns Comm'n [FCC], *Connecting America: The National Broadband Plan* ch. 4 (2010).

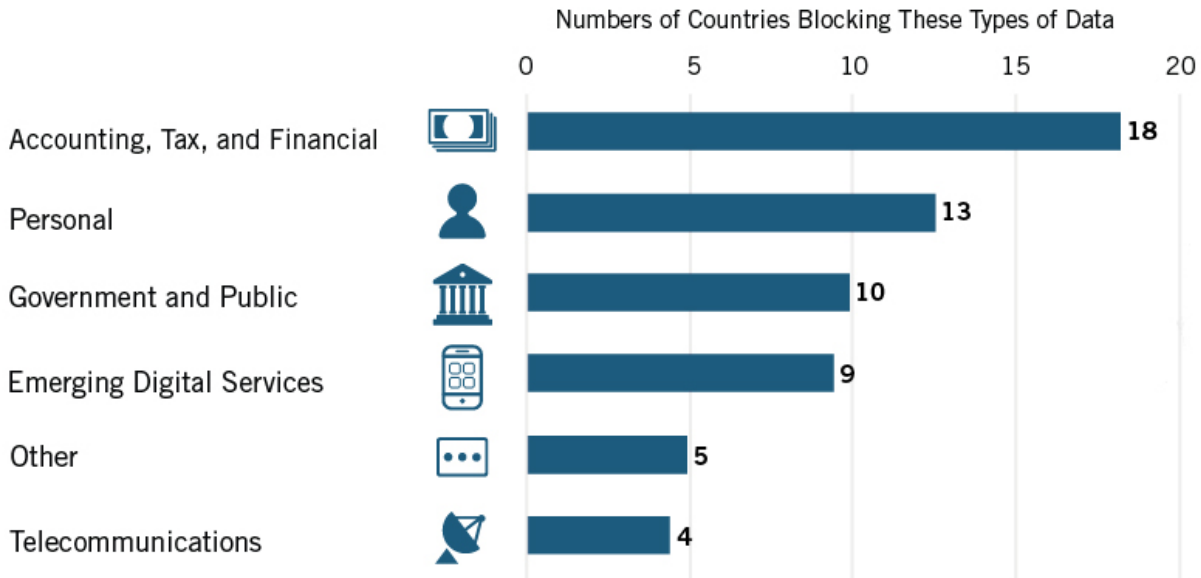
Blocking the Global Flow of Data

Which Countries Block Data Flows?*



No data blocked
1-2 types of data blocked
3+ types of data blocked

What Types of Data Are Blocked?*



**ITIF analysis of formal laws or regulations publicly reported as of April 2017.*

ITIF
INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Learn more at itif.org/databarriers

Data Localization Snapshot Current as of January 19, 2017

Active Measures		
Country	**Measure**	**Details**
Australia	Personally Controlled Electronic Health Record Provision	This regulation restricts the exportation of any personally identifiable health information.
Canada	Two provincial personal information laws: Nova Scotia and British Columbia	These two provincial laws restrict the exportation of any personal data collected by or for public bodies.
China	Cyber-Security Law	This law contains broad requirements for local processing and storage of "important data" related to Chinese citizens and critical information infrastructure.
China	Notice to Urge Banking Financial Institutions to Protect Personal Information	This law prohibits the off-shore analyzing, processing, or storage of Chinese personal financial information.
China	Guidelines for Personal Information Protection within Public and Commercial Information Systems	This standard prohibits the overseas transfer of data without express user consent or government permission.
China	Online Publishing Service Management Rules	This law requires that all servers used for online publishing in China be located within China.
China	Population and Healthcare Information Management Measures	These measures prohibit the overseas transfer of health and medical information.
Germany	Telecommunications Act	Amendments to this act require telecommunications providers to store meta data for a specified period of time within the borders of Germany.
India	National Data Sharing and Accessibility Policy	This policy requires all data collected using public funds to be stored within the borders of India.
Indonesia	Regulation No. 82: Information and Electronic Transaction Law	This law mandates that any company which provides internet enabled services directly to the consumer must locate their data centers within Indonesia.
Kazakhstan	Amendments to Certain Legislative Acts on Informatization	These amendments require that all personal data collected within Kazakhstan be stored within the country.
Korea	Act on the Establishment and Management of Spatial information	This act, an update to a law which originated in the Korean War era, greatly restricts the cross-border transfer of mapping data.
Nigeria	Guidelines for Nigerian Content Development in ICT	These guidelines require that all consumer and subscriber data collected by companies in Nigeria be hosted within Nigeria.
Russia	Federal Law 242-FZ	This law requires that all data collected on Russia citizens be stored within Russia.

Russia	Federal Law 149-FZ	This law: 1) Requires any organization which "disseminates" information on the internet (email, messaging services, etc.) must keep all metadata within Russia for 6 months; and 2) all bloggers with more than 3,000 followers must register with local authorities.
Turkey	E-Payment Law	This law requires companies that provide e-payment services to conduct all data processing within the borders of Turkey.
United States	DoD Interim Rule on Network Penetration Reporting and Contracting for Cloud Services	These rules require that all cloud computing service providers that work for the DOD to store DOD data within U.S. Territory.
Vietnam	Decree of Information Technology Services	This law mandates that all companies that provide a range of different internet enabled services maintain at least one server within the borders of Vietnam.

Potential Measures

Country	Measure	Details
China	Draft Supervision Rules on Insurance Institutions Adopting Digitized Operations	This law would require localization of data servers by any insurance institution processing the personal data of Chinese citizens. Additionally, there are vague requirements for data residency that are yet to be defined.
China	Secure and controllable standards	In addition to highly invasive IP disclosure requirements, the regulation also has a section that gives preferred status to companies that can have upfront design duplicated environment of CPUs located within China.
Indonesia	Draft Regulation Regarding the Provision of Application and/or Content Services Through the Internet	This law has a vague requirement that OTT service providers place part of their data centers within Indonesia.
Korea	Standards for Cloud Computing Services	These pre-announced standards would require all cloud computing providers place servers handling public data within the borders of Korea.
Saudi Arabia	Proposed Regulation for Cloud Computing	This proposed regulation would require cloud service providers to store certain types of data locally based on a four tier data classification system.
Vietnam	Draft OTT Circular	This draft law would require all OTT service providers to locate at least one server in Vietnam.

INNOVATION ECONOMY

Emerging Internet Technologies: Internet of Things and Machine Learning

FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS

THE DEPARTMENT OF COMMERCE
INTERNET POLICY TASK FORCE &
DIGITAL ECONOMY LEADERSHIP TEAM
January 2017

1. Executive Summary

The Internet of Things (IoT) – in which connected devices are proliferating at an unprecedented rate – is a technological development that is transforming the way we live and do business. IoT continues the decades-long trend of increasing connectivity among devices and the Internet, bringing online everything from refrigerators to automobiles to factory inventory systems. At the same time, IoT encompasses a widening scope of industries and activities and a vastly increasing scale and number of devices being connected, thus raising the stakes and impacts of broad connectivity.

The prospective benefits of IoT to personal convenience, public safety, efficiency, and the environment are clear. IoT has the potential to make our highways safer by enabling connected vehicles to interact with each other to prevent accidents, to make quality health care more accessible through remote monitoring devices and telehealth practices for those who cannot easily travel, and to reduce waste and improve efficiency both in factory supply chains and in the running of cities. It even has the potential to create new industries and consumer goods that have yet to be imagined. For the full potential to be realized, however, the necessary infrastructure and policies must be in place, including strategies to respond to the challenges raised in areas such as cybersecurity and privacy.

Due to its expertise in the issues raised by IoT, as well as its economy-wide perspective, the Department of Commerce (Department) is well placed to meet these challenges and to champion the development of a robust IoT environment that benefits consumers, the economy, and society as a whole.

With an April 2016 Request for Comment, "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things,"[1] the Department of Commerce sought to review the current technological and policy landscape relating to IoT**.** A broad array of stakeholders – from the private sector, academia, government, and civil society – offered perspectives[2] in response to the request. In September 2016, the Department hosted a workshop[3] to delve deeper into the questions raised by the Request for Comment, and to explore some of the related issues arising from the public comments.

This paper represents the Department's analysis of those comments. It also identifies key issues that can impact the deployment of IoT technologies, highlights potential benefits and challenges, and discusses what role, if any, the U.S. Government, particularly the Department of Commerce, should play in this evolving landscape.

---

[1] *See* https://www.federalregister.gov/d/2016-07892

[2] *See* https://ntia.doc.gov/federal-register-notice/2016/comments-potential-roles-government-fostering-advancement-internet-of-things

[3] *See* https://ntia.doc.gov/other-publication/2016/09012016-fostering-advancement-internet-things-workshop-webcast

Over the past few decades in the United States, the role of government largely has been to establish and support an environment that allows technology to grow and thrive. Encouraging private sector leadership in technology and standards development, and using a multistakeholder approach to policy making, have been integral elements of the government's approach to technology development and growth. Following a review of public comments, meetings with stakeholders, and the public workshop, it is clear that while specific policies may need to be developed for certain vertical segments of IoT, the challenges and opportunities presented by IoT require a reaffirmation rather than a reevaluation of this well-established U.S. Government policy approach to emerging technologies.

The goal of this paper is to identify elements of an approach for the Department of Commerce to foster the advancement of the Internet of Things. The record of comments underlying this green paper, however, does set forth a series of issues that should be considered in any future discussions related to the possibility of a national IoT strategy. The Department heard a strong message from the submitted comments that coordination among U.S. Government partners would be helpful, because of the complex, interdisciplinary, cross-sector nature of IoT. A federal coordination structure for these issues may also be helpful when working with international and private sector partners.

This paper begins with an overview of IoT, including definitional issues, the benefits of IoT, the possible role of government in fostering the IoT environment, and some of the international considerations that, due to the global nature of the Internet and connected technologies, are inherent in the issues discussed in the rest of the paper. The next section lays out an approach for Departmental action organized around four engagement areas. The section thereafter provides a review and analysis of the comments, current Department initiatives, and next steps for each engagement area. Consistent with the established U.S. Government policy approach to emerging technology, this approach proposes the following principles:

- The Department will lead efforts to ensure the IoT environment **is inclusive and widely accessible** to consumers, workers, and businesses;
- The Department will recommend policy and take action to support a **stable, secure, and trustworthy** IoT environment;
- The Department will advocate for and defend a **globally connected, open, and interoperable** IoT environment built upon industry-driven, consensus-based standards; and
- The Department will encourage IoT **growth and innovation** by encouraging expanding markets and reducing barriers to entry, and by convening stakeholders to address public policy challenges.

The approach identifies four broad areas of engagement to advance these principles:

- **Enabling Infrastructure Availability and Access:** Fostering the physical and spectrum-related assets needed to support IoT growth and advancement.
- **Crafting Balanced Policy and Building Coalitions:** Removing barriers and encouraging coordination and collaboration; influencing, analyzing, devising, and promoting norms and practices that will protect IoT users while encouraging growth, advancement, and applicability of IoT technologies.
- **Promoting Standards and Technology Advancement:** Ensuring that the necessary technical standards are developed and in place to support global IoT interoperability and that the technical applications and devices to support IoT continue to advance.
- **Encouraging Markets:** Promoting the advancement of IoT through Department usage, application, iterative enhancement, and novel usage of the technologies; and translating the economic benefits and opportunities of IoT to foreign partners.

The approach proposes engagement on a set of cross-cutting issues across these contexts from cybersecurity and privacy to innovation and intellectual property, with all stakeholders at the local, tribal, state, federal, and international levels. The green paper delves in depth into each of these areas of engagement, summarizing commenter feedback, describing current DOC initiatives, and proposing next steps (summarized in Appendix A: Proposed Next Steps).

The publication of this green paper will be followed by a further Request for Comment that will solicit feedback on the findings of the paper and the proposed approach and next steps. This further consultation will inform the Department's approach and next steps as we work with interagency partners on the U.S. Government's approach to IoT.

An Introduction to Artificial Intelligence and Machine Learning

Artificial intelligence (A.I.) is no longer the realm of science fiction but a practical software tool used to help millions of people every day. This has been driven by recent breakthroughs in the field of machine learning, a branch of artificial intelligence that specifically studies algorithms which learn and improve from training examples. While these developments have been decades in the making, they are only now becoming practical because of the availability of computational power, richer sources of information, and a growing community of talent across the globe.

Machine learning is powering a variety of existing Google products aimed to support user protection (e.g., spam and malware filters), accessibility and access to knowledge (e.g., voice recognition and translation) and improve search (e.g. image recognition in photos).

Machine learning is creating opportunities for entirely new products as well. For example, Google Assistant leverages machine learning tools across different dimensions: speech recognition turns the sounds into words, natural language processing helps understand what you mean, and a type of deep learning helps rank search results.

Beyond simply opening opportunities for the next generation of products, we also think that machine learning can be used to tackle some critical public challenges. We also recently announced that machine learning is helping to reduce the environmental impact of our data centers[1] and can be used to augment the quality of medical diagnosis[2].

Economic and Societal Impact and Key Industries

Bank of America Merrill Lynch estimates A.I. solutions market will grow to US$153bn by 2020, comprising US$83bn for robotics, and US$70bn for A.I.-based analytics[3]. The report also suggests that the adoption of A.I. and automated tools could boost productivity by 30% in many industries, while cutting manufacturing labour costs by 18-33%. Asia-Pacific is expected to account for the highest CAGR in the field during the period[4].

A.I. will have an overarching impact on different industries and spheres of life. For example, In retail, machine learning algorithms behind Amazon or Alibaba are aimed at driving greater customization, user engagement and personalization of the shopping experience.

From better navigation and assistance to self-driving vehicles, A.I. is expected to not just revolutionize human transit and cargo shipment but ultimately facilitate safer, cheaper and more environmentally friendly means of transportation for industry and consumers.

In agriculture, artificial intelligence and machine learning tools will continue to drive productivity and efficiency of human labour thanks to automation of routine processes, and can also help increase the accuracy of analysis of a number of factors ranging from soil conditions to historical weather patterns aimed at forecasting the impact of climate change or natural disasters. Multiple examples across the globe already demonstrate this capacity: Australian farmers are training 'farmbots' to herd livestock and keep an eye on their health[5], Indian startups are using machine learning to identify areas most affected by changing climate conditions[6], and an enterprising cucumber farmer in Japan has found a way to use machine learning and Google's open source platform TensorFlow to automatically sort cucumbers by size, shape and other attributes to raise productivity on his family farm[7].

The impact of A.I. and machine learning technology on health care and quality of life in the long term will probably be the most beneficial for society. Take for instance diabetic retinopathy, a common complication of diabetes and one of the fastest growing causes of blindness globally. It can be prevented if detected early but the problem is, especially in developing countries, that there are not enough ophthalmologists to provide screening and diagnostics (there are over 380 million diabetics worldwide who should be screened annually — and only 200 thousand ophthalmologists). Our research shows[8] that machine learning can make the diagnosis of diabetic retinopathy more broadly accessible. Other Alphabet companies, including DeepMind and Verily, are working on different types of research aimed at improving diagnosis, prevention and treatment of diseases with the help of A.I. and machine learning. And there are many more examples from the global medical research community: for instance U.S. radiologists have most recently published a paper on adapting TensorFlow to identify signs of Parkinson's disease in medical scans[9]. Apart from enhanced diagnosis, artificial intelligence and machine learning tools can help improve efficiency of designing treatment plans, medication management or provision of better care for the elderly population through smart assistance and automated support.

Application of machine learning tools in a broader range of sciences is endless. Take for instance the experience of Australian marine biologists who are using TensorFlow to find sea cows[10] in tens of thousands of high resolution photos to better understand their populations, which are under threat of extinction.

In education A.I. can help address learning challenges with smart assistance and content customised to individual learners. Online courses, with video lectures, discussion boards for students and systems to grade their coursework automatically, otherwise known as Massive Open Online Courses (MOOCs), are already an important addition to existing university teaching and a great help for distant learners. In the years to come artificial intelligence could play a role in growing the field of learning analytics, and evaluating the quality of curricular materials.

Another area where we are continuously experimenting with A.I. and machine learning technology is arts and culture. Google Magenta

1) https://goo.gl/BymdCR
2) https://goo.gl/ySaogF
3) https://goo.gl/OSMdoQ
4) https://goo.gl/OI7YmK
5) https://goo.gl/40cRRz
6) https://goo.gl/R5QUeX
7) https://goo.gl/4l7IbF
8) https://goo.gl/fEfWvf
9) https://goo.gl/m3JkbM
10) https://goo.gl/7WQ3gp

is a research project aimed at building smart new tools for artists and creators to advance the state-of-the art in music, video, image and text generation using machine learning and artificial intelligence tools, and is ultimately an attempt to build a community of technically-minded artists, coders and machine learning experts experimenting with the emerging computing technology and specifically neural networks.

Machine learning is also demonstrating a capacity to make electrical and other systems more energy-efficient and thus tackle one of the world's most challenging physical problems - energy consumption and climate change. Reducing energy usage has been a major focus for Google over the past 10 years, and considerable progress has been made on this front through our own super-efficient servers and new ways to cool our data centres with the goal of being powered 100% by renewable energy. However a major breakthrough occurred earlier this year, when application of DeepMind's machine learning to Google data centres allowed us to reduce the amount of energy we use by up to 40 percent[11]. These implications are significant not only for Google's data centres but have a potential to greatly improve energy efficiency and reduce emissions for other companies who run on Google's cloud. Similar technologies are turning the dream of "smart" homes into reality, lowering energy bills and tackling climate change.

Moreover, A.I. and machine learning tools could be broadly implemented to help preservation and sustainability of existing ecosystems, an important consideration in many developing economies. For example, researchers in Brazil have used neural networks to fight deforestation by developing more accurate measures of tree taper - a critical variable in estimating forest density and health[12]. A neural network is able to better analyze the many variables in tree density found in tropical rainforests to improve sustainable forestry initiatives, such as identifying areas for timber production and preservation.

These are just some of the examples, and we are excited to see the scientific community study and deploy these technologies in different fields.

Responsible Development of A.I.

While the recent pace of development has been rapid, neither the advancement of machine learning nor its impact on society is preordained. We need to address several issues in order to maximize the benefits of this technology for everyone.

Google is focused on three near term challenges that we believe need to be made a priority. We trust that positive work in these areas will help machine learning advance and see even more widespread application over the next five to ten years.

Preserve Open Research Norms and Practices. Machine learning has flourished in part because of a set of common norms that encourage research results to be published and shared openly. It is important to preserve these community principles. Google has been an active contributor to the research community globally. We publish results of our research[13], actively participate in the world conferences on a variety of topics in the field and bring visiting faculty, PhD students and interns from all over the world to Google as well as give large grants to over 250 academic research projects every year. Last year we open sourced TensorFlow - Google's internal machine learning toolkit - to help researchers and developers from all over the world to experiment in the space and advance the state of the art. We have already seen a number of inspirational examples of adoption of these open source tools in different industries from medical research to farming and by a variety of SMBs[14]. In order to further support the research community, DeepMind has also published the game moves from AlphaGo's games supplemented by the expert commentary, available in different languages[15]. We will continue this work and encourage other researchers globally to follow this practice of commitment to openness.

Dedicate Research to Safety and Ethical Development of Machine Learning. As with any technology, it is important to maximize the positives and minimize concrete harms. The rapid advance of the field of machine learning has raised concerns surrounding the safety of implementing these systems in a variety of different contexts. Alongside this has been the recognition that machine learning systems trained on biased data may themselves render biased or discriminatory outcomes, or that such systems, by focusing on more objective criteria, might help reduce or avoid discrimination. No system is perfect, and errors will emerge. However, advances in our technical capabilities will expand our ability to meet these challenges. To that end, we believe that solutions to these problems can and should be grounded in rigorous engineering research to provide the creators of these systems with approaches and tools they can use to tackle these problems. "Concrete Problems in A.I. Safety"[16], a recent paper from our researchers and others, takes this approach in questions around safety. We also applaud the work of researchers who along with Moritz Hardt at Google Brain are looking at questions of bias and discrimination and approaches to correcting algorithmic bias[17]. To support an open collaboration on the best practices of responsible A.I. development, Google has taken part in establishing a new cross-industry Partnership on AI[18] which is aimed at addressing opportunities and challenges with A.I. technologies to benefit people and society. The partnership will conduct research and recommend best practices in areas such as ethics, fairness and inclusivity; transparency, privacy, and interoperability; reliability and robustness of the technology, and others. This is a collaborative and multi-stakeholder organization, and we hope it will spur a dialogue across the research community globally. Similarly, there is a growing need for dedicated training courses on ethical and responsible development for researchers in the field. And universities and academic community globally should play an active role in implementing this approach and adjusting relevant curriculums.

Diversify the Community Adopting Machine Learning. Machine learning can produce benefits that should be broadly shared throughout society. Having people from a variety of perspectives, backgrounds, and experiences working on and developing the technology will help us to identify potential issues. Continued investment in computer science education will help support this goal. Google is working to expand computer science education in a way that engages and retains students from all backgrounds. This includes programs that increase access and exposure, including initiatives like CS First, Made with Code, Exploring Computational Thinking, and the Computer Science Summer Institute, and our support of innovative organizations through the RISE Awards. Broad dissemination of the knowhow around machine learning is critical as well, since it provides resources for anyone interested in learning more. But this collaboration should go beyond research and engineering community alone. As we continue developing A.I., new questions will continue to arise, and we will need to answer them with the involvement of a broader range of stakeholders including academia and civil society,

11) https://goo.gl/zAenvV
12) https://goo.gl/jHds2j
13) https://goo.gl/jSMBXO
14) https://goo.gl/W6vhsm
15) https://goo.gl/k6vT1h
16) https://goo.gl/t8AjLH
17) https://goo.gl/ZHyaSf
18) https://goo.gl/H8JFZs

policymakers, experts from business and public sectors, in particular, those industries that will be impacted the most as a result of advances in A.I. and machine learning. All these stakeholders need to be part of a global conversation.

What Policymakers Can Do

A broader understanding of the technology is an important part of appropriately identifying opportunities where machine learning will have the biggest and most positive impact. We believe that government has a significant role to play in catalyzing research and efforts that meet the challenges outlined above and in promoting the development and application of these technologies.

Here are some examples and focus areas we believe are crucial for government and private sector collaboration in this emerging field

Support research

Governments across the world have traditionally played an important role in supporting long-term fundamental research. The government has and should continue to play that role with machine learning, supporting research into the novel application of these technologies in meeting social challenges and addressing potential limits and shortfalls. Supporting international education and exchange programmes for researchers and the engineering community will constitute a big part of this effort as well.

Convene talent to meet social challenges and support a multi-stakeholder approach

Machine learning has proven to be an effective tool for making progress on complex problems on a significant scale aimed at addressing global challenges in fields like energy, transportation, environment, urban planning, and public health. Therefore increasing dialogue between the public and private sectors, including the academic community, researchers, tech industry leaders, government, and representatives of NGOs and civil society will be crucial to this process. We believe that governments can convene cross-sectoral task forces at a national level to ensure an informed multi-stakeholder approach to development of best practices in the area with participation of the industries most impacted by the emerging tech.

Exchange best practices and support international dialogue

Machine learning is an international phenomenon, drawing on researchers and datasets from around the world. Successful development of machine learning depends on the continuation of pro-innovation legal regimes in different interconnected fields from ICT policy to digital economy or copyright, where flexible, well designed limitations and exceptions can spur the development of new technologies. A multi-stakeholder approach is crucial not only at a national level but also as part of the international dialogue, and we believe governments across the world could amplify fora like G7 or G20 as well as intergovernmental platforms such as the OECD and others to exchange best practices and formulate a consistent international approach to innovating policy and legal frameworks aimed at supporting A.I. and machine learning development globally.

Support data driven innovation and liberating data flows

Data-based training examples are an important ingredient in machine learning, and hence government policies supporting data driven innovation and encouraging open data standards would facilitate algorithmic training and help correct bias. Particularly where these systems are deployed in public administration, we believe the government and the international community can and should promote the release of high quality and robust datasets that enable responsible analysis and use. Privacy and data protection experts on the government and industry side should work in collaboration to ensure proper standards are in place that will guarantee protection of the rights of individuals and institutions to privacy and control over their personal data as part of this process.

Promote Education and Diversity

Governments all over the world should encourage increasing access to and diversity in STEM education and careers. We should continue this effort to ensure that more students from more backgrounds have access to computer science education. Public and private sector partnerships are crucial to advance this effort, and Google has traditionally taken an active approach and designed multiple programs globally to support STEM education. With increased progress in robotics and automation and new challenges arising from these technological advances, innovative training and re-training programmes should be developed in close cooperation between government and the industry to address the future impact of automation on the structure of labour market and support the transition across different geographies.

Ensure Flexibility

Despite many recent breakthroughs in machine learning, the field and its applications are still nascent. As these opportunities are still emerging, we encourage a cautious and nuanced policy approach that will allow innovative uses to flourish and reach their full potential. We also believe consensus driven best practices and self-regulatory processes will play an important role in ensuring the flexibility necessary to drive innovation while simultaneously developing appropriate safeguards.

Conclusion

Though we are at a very early stage of this exciting journey, A.I. and machine learning technologies are already a reality providing better tools for humans and improving our everyday life. Our vision is to advance these tools within our products that will assist people in better and smarter ways, give them more choices, and ultimately help address the world's bigger and more complex challenges across different sectors. We believe this is a collaborative process which relies upon open research, exchange of best practices and continuous multi-stakeholder dialogue which we are committed to further supporting.

INTERMEDIARY LIABILITY PROTECTIONS: A CORNERSTONE OF THE INTERNET'S SUCCESS

INTERNET PLATFORM ENABLERS:
Laws that Protect Speech & Creativity

Internet Association

Online Platforms Drive Economic Growth

Online platforms- like Airbnb, Amazon, Facebook, Google, LinkedIn, Twitter, and Yahoo!- underpin how the Internet works; they boost commerce and increase opportunities for businesses by allowing anyone, anywhere, to connect with billions of people to access and share information.

The ability of U.S. based Internet platforms to host user-generated content has fueled crucial free expression and content creation both at home and around the world. It has led to the creation of a booming domestic Internet economy. In the past few years, Internet platforms have fundamentally revolutionized and improved the way we use transportation, purchase goods and services, and facilitated the exchange of ideas.

Lower barriers to entry

$967 Billion
6% of GDP

Smart laws allow responsible online platforms to operate at scale.

These laws ensure platforms are not responsible for their users' actions if the platforms act responsibly and meet certain reasonable conditions. This includes removing content when they are given notice.

Without these laws:

Online intermediaries could be forced to censor user activity, including political speech and consumer commentary, online to avoid costly litigation. Users' ability to access real time content would be drastically limited by the motivation to review content.

Websites would have to have teams of lawyers devoted full time to fighting lawsuits and monitoring user content.

Because of expensive lawsuits, the barriers to entry for Internet startups would rise drastically and prevent new, creative services from ever being started.

Keep the Balance in Smart Laws: There are constant proposals to disrupt the carefully struck balance to make online platforms more liable for their users' content, however, doing so would fundamentally alter the internet ecosystem in ways that would hinder economic growth and other core values such as free expression.

- If digital content intermediaries were responsible for the content uploaded by users, **81-85%** of investors would be **less likely to help startups**.[1]
- Proposed changes to liability may reduce investment more than an economic recession: **85% of investors are uncomfortable as investors** in digital content intermediaries open to unpredictable regulation.[2]
- **Proposals to make platforms 'Internet cops' will reduce free expression**. If online platforms were to be held responsible for content submitted by their users, they would likely remove large amounts of controversial but legal content, for fear of facing penalties. These proposals would also threaten important balanced provisions of copyright law, including fair use, which is critical to the functioning and development of technology and services.

[1] Engine Study & Booz Study

[2] http://engine.is/wp-content/uploads/EngineFifthEraCopyrightReport.pdf

The Balance in Law Allows Internet Platforms to Operate at Scale

Support continued free expression and First Amendment rights by maintaining the Communications Decency Act Section 230.

Section 230 of the Communication Decency Act of 1996 was passed to protect online services from being held responsible for user speech and content, **ensuring a robust Internet ecosystem that promotes free expression and innovation.**

Section 230 relieves these intermediaries from limiting user speech in order to limit legal pressures, **paving the way for diverse Internet platforms.**

Continue to provide opportunities for creators, nurture innovation, and give enjoyment to consumers by maintaining Section 512 Safe Harbors of the Copyright Act.

Section 512 of the Copyright Act creates conditional safe harbors for responsible online platforms that limited liability for copyright infringement, which allows platforms to **flourish with legal certainty and clarity**.[3]

The safe harbors are innovation enablers

Online platforms have **enabled immense growth and opportunities for creators of all backgrounds**. Digital is currently driving growth in the content industry; it accounts for the majority of music revenue, and movie-streaming services are growing at 28% and will exceed physical sales by 2018.[4]

The production of culture and media is on the rise in the U.S., particularly digital content.[5]

U.S. consumers prefer online media and get an additional $970 in value – called the 'consumer surplus'- beyond what they pay to access it each year.[6]

[3] Section 230 specifically excludes intellectual property infringement.
[4] PwC, 'Global entertainment & media outlook 2014-2018', 2015, http://goo.gl/APtAMh
[5] (Floor64, 'The Sky is Rising', 2012,https://goo.gl/0TF1BV)
[6] (BCG, Follow the Surplus', 2013, https://goo.gl/m7CmNT)

THE DIGITAL SINGLE MARKET AND A DUTY OF CARE: PRESERVING THE TRANSATLANTIC LEGAL FOUNDATION OF A THRIVING INTERNET

by DANIEL O'CONNOR *on* JULY 9, 2015

As part of the Digital Single Market (DSM) communication, the European Commission has discussed the possibility of imposing a "duty of care" on Internet intermediaries, which would require Internet platforms to take a more active role in policing user content. Forcing Internet intermediaries to monitor and remove their users' communications is ill-advised from both an economic and human rights standpoint.

The rapid growth of the Internet was not merely the function of technological innovation. This fundamental restructuring of commerce and communications would not have been possible but for substantive legal reforms that adapted legacy legal concepts to comport with the realities of a hyper-connected Internet age. Arguably the most important legal and legislative development of the Internet era was the concept of intermediary liability limitations for Internet service providers. Or, stated in a less legalistic way, the policy choice that Internet services should not bear blame for bad people saying or doing bad things on the Internet. Given the size and scope of the Internet and the volume of online communications, it is safe to say that Facebook, Twitter, Google, Yelp, YouTube, Allegro, and Dailymotion would not exist today if the law evolved to hold websites and Internet services liable for the actions of their users. Further, imagine operating a telecommunications network with the sum of all this information passing through without being shielded from responsibility for the actions of all of your users. What venture capitalist in her right mind would invest in a platform that was exposed to liability for billions of websites beyond its control or trillions of posts composed by third parties? What would Internet business models look like if companies had to pre-screen all user communications before they went live?

Recent developments in Europe, including the Delfi ruling and the DSM "duty of care" proposal, suggest that Internet services may soon be asked to take a more active role in filtering user content. Yet even with advanced filtering tools, unlawful speech is almost always context dependent. Libel and defamation would not be obvious to a filter. Even more complex is when lawful speech is used unlawfully, as in the case of copyright and trademark infringement. Given that rules about these various types of speech are often the product of complex legal cases, even human review of every online communication would not completely

shield an Internet company from liability, given that different people can come to different conclusions about whether speech is "harmful." Not to mention that standards for what is permissible speech vary widely from country to country.

Besides the commercial impact, the implications for free speech would also be disastrous. Protections from intermediary liability enable platforms to give people around the world a simple way to express themselves and to share what they love with the world, and to challenge the restrictions of oppressive governments. One study found that when online platforms are regulated on the basis of content submitted by their users, they remove large amounts of controversial but legal content for fear of facing penalties. The UN's Joint Declaration on Freedom of Expression on the Internet recognizes the success of laws such as the CDA, DMCA, and the E-Commerce Directive, stating that "intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression."

Even if pre-screening and filtering at scale were feasible, the value of each individual communication — whether it takes the form of a website, a tweet, a Facebook post or a YouTube video — is negligible, where the potential legal exposure is huge; the potential damages for copyright law can reach $150,000 *per work infringed*. So, in a world where Internet companies were liable for the communications of their users, a rational company would be incentivized to aggressively censor content, leading to significant blocking of ostensibly legal speech as the costs of under blocking are significantly more than the costs of over blocking.

Historical Context on Intermediary Liability

Initially, the legal status of Internet companies was uncertain. Problematic cases arose where the courts found Internet companies liable for user-generated content. However, both the United States and the European Union were relatively quick to act. In the United States, Congress passed Section 230 of the Communications Decency Act in 1996, which shielded Internet service providers from liability for a variety of actions that were committed by their users. Although §230 specifically did not include intellectual property infringement, Congress passed the Digital Millennium Copyright Act in 1998, which shielded Internet platform providers from liability for their users' infringement provided they acted quickly to remove infringing content when notified. In the subsequent report that accompanied the bill, the Senate Judiciary Committee made clear that these intermediary liability provisions were necessary given that the size and scope of the Internet made it functionally impossible for Internet service providers to monitor all the material that they served or indexed. At the time, Yahoo!, the illustrious example used by the Committee, indexed 800,000 websites. Counting just websites, and not other forms of content on social media, the number of sites Yahoo! indexed in 1998 was less than 0.1% of the size of the current web. As new Internet entrepreneurs seek to join the Yahoos, Twitters, and Facebooks of the world, it is imperative that those companies are afforded the same legal protections that allowed the prior generation of Internet success stories to achieve scale.

Europe was also quick to embrace the concept of liability limitations. In 2000, the European Union adopted the e-Commerce Directive, which endorsed a similar notice-and-takedown framework of Internet service providers for most Internet content. Since it was a directive that needed to be interpreted by individual European countries, it resulted in some inconsistency of application that provided somewhat less certainty to Internet companies than the U.S. versions of Intermediary liability. Nevertheless, it has provided the necessary legal foundations for the Internet to grow and expand in Europe.

These laws do not create any general monitoring or filtering obligations for illegal or harmful content. US law states that a service provider need not monitor its service or seek out infringing activity in order to qualify for the DMCA safe harbor. (This provision is intended to protect user privacy. Without safe harbors in place, website administrators might be required to search through and peer into their users' otherwise hidden conversations.) Under the e-Commerce Directive, states may not impose general obligations on intermediaries to monitor information or to actively seek out unlawful activity.

If any reform of the e-Commerce Directive is needed, it should be in the direction of giving EU startups and platforms *greater* assurance that they will not be found liable for the speech of their users. Adopting a liability regime closer to §230 would provide a critical boost to the growth and global competitiveness of EU communications platforms, review sites, social media platforms, dating apps, e-commerce sites, and the next generation of digital innovators.

Intermediary Liability Enables Flexible Responses to Harmful Content

The existing rules in place in the US and EU have led to strong respect for rights. Internet platforms already take down a significant amount of content that infringes copyright. In addition, platforms respond to court orders and cooperate with law enforcement on issues like child sexual abuse imagery. Finally, while there's no one-size-fits-all solution to the problem of online abuse, many platforms have evolved highly effective community policing and report abuse systems that help stop the spread of harassment, hate speech, and other harmful content. For example, anyone on YouTube can flag a video for review, and Google employees review those flagged videos for abuse 24 hours per day. In 2014, 14 million videos were removed from YouTube for violation of the site's Community Guidelines. (Twitter and Facebook also have similar guidelines and flagging procedures that can lead to removal of content and the termination of accounts.)

Unfortunately, as part of its DSM initiative, some are calling for a re-opening of the e-Commerce Directive and implementing a new "duty of care" on Internet service providers. This "duty of care" would be effectuated by either narrowing, or completely removing, the liability safe harbors available to Internet companies under the e-Commerce Directive. According to the Staff Working Document that accompanied the DSM communication, the European Commission noted that it was considering "whether to enhance the overall level of protection from harmful material through harmonised implementation and enforcement of conditions which allow online intermediaries to benefit from the liability exemption." Furthermore, as part of this examination, the Commission is also asking "whether to ask intermediaries to exercise greater responsibility and due diligence in the way they manage their networks and systems... so as to improve their resistance to the propagation of illegal content."

The same document also acknowledges that the intermediary liability safe harbors included in the e-Commerce Directive "underpinned the development of the Internet in Europe." Let's hope this last statement is borne clearly in mind if any updating takes place, remembering that a consistent process across Europe could be useful, but that a weakening of the liability shield and an extension of proactive monitoring would be economically and socially disastrous.

Economic Effects of a "Duty of Care"

The ramifications for future competition and innovation are also dire if the European Union were to enact a broader duty of care provision for Internet intermediaries. Given the limitations of automatic filters, and the

fact that harmful, illegal content is context dependent, new online companies that offer communications platforms will need to employ large teams of human filters to review user-generated content.

What does that mean for competition and innovation? It likely means that startups and new business models will be disproportionately affected. From a venture capital perspective, the imposition of new regulatory costs on traditionally lean startups means that fewer new ideas get funded. Given that Internet platforms often spend years developing a user base before they devise ways of turning their popularity into revenue, the added costs will also mean that many of these ideas either don't get funded, run out of money before achieving the necessary scale, or simply prove unable to turn a profit.

The companies best positioned to bear these new cost burdens are the current Internet incumbents who have large legal departments and significant revenue. And depending on how new regulation might be written, even a large number of human reviewers still cannot catch everything. The number of humans needed to review 500 million tweets a day or 1 trillion Facebook posts is mind-boggling. In the YouTube example alone, 300 hours of video uploaded per minute makes 18,000 hours per hour or 432,000 hours per day. That would require non-stop oversight from *18,000* people to vet everything–and that's assuming they never get a day off and never sleep. (Not to mention, this makes it harder to push back against laws from more authoritarian regimes demanding the censorship of "harmful information".)

Higher regulatory and legal burdens threaten the robust competition and disruptive innovation that has characterized the Internet ecosystem over its short history. High regulatory costs entrench incumbents. This could disproportionately affect European companies, as none of the top 15 global Internet companies are European. However, Europe does have a high-share of the so-called "unicorns" — startups that are valued at more than $1 billion. (And, according to a recently released study, the unicorn population of Europe grew by 13 between 2014 and 2015.) Furthermore, nearly one quarter of the startups at the 2015 Consumer Electronics Show were French! As higher regulatory burdens harm smaller companies more than large ones, such an imposition of regulatory costs hurts these plucky startups more than the Googles and Facebooks of the world.

Increasing Liability Would Harm Startups, SMEs and the Broader European Economy

Imposing a duty of care on Internet services wouldn't just harm new startups in the EU. As we have discussed before, the Internet has transformed the world's economy and spurred economic productivity. The majority of these benefits accrue to traditional industry, not "Internet companies," through streamlining logistics and reducing frictions in international commerce. In fact over the last 20 years, the U.S.'s greater economic productivity growth relative to Europe has been powered by its the better integration of Internet and networked technology into the overall economy. Given the role Internet platforms have played in this economic transformation, creating legal frameworks that enable the creation and foster the growth of Internet platforms — such as social media, e-commerce, financial services, crowdfunding, cloud computing, advertising, etc. — is important not just for the Internet sector, but for the broader economy that relies on them to enable their day-to-day business operations.

Not surprisingly, small and medium size businesses often benefit the most from these platforms, as Internet platforms enable them to immediately build infrastructure, conduct traditional back office operations, take payments, easily target advertising to prospective consumers, and reach consumers worldwide through e-commerce platforms in ways that were not possible before the rise of Internet commerce. With this in mind, it's not surprising that SMEs who heavily utilize that Internet are 10% more productive (and export two times

as much products and services) as companies that do not. Also not surprisingly, SMEs were the key to the U.S. economic and jobs recovery, and are seen as key to powering the European economic recovery. As European policymakers sit poised to decide the nature and scope of Internet regulation as part of the Digital Single Market (DSM) initiative, creating a legal and regulatory environment for Internet platforms to thrive (and new ones to be created) should be a top priority. Ensuring that robust online intermediary liability protections extend across the European Union stands as arguably the most important policy imperative of the DSM if Europe wants its vibrant, connected digital economy to thrive in the 21st century.

If anything, for the Internet to continue to grow and thrive, liability limitations for online companies should be expanded and strengthened. It is a worthwhile and important endeavor for the European Commission to clarify and harmonize liability safe harbors across Europe. However, harmonization with a weakening of these safe harbors will have negative effects for both freedom of expression and Internet commerce.

Tagged as: Digital Single Market, DSM, Duty of Care, EU, European Commission, Intermediary Liability

BALANCED COPYRIGHT: FAIR USE AND OTHER KEY CONCEPTS IN U.S. LAW

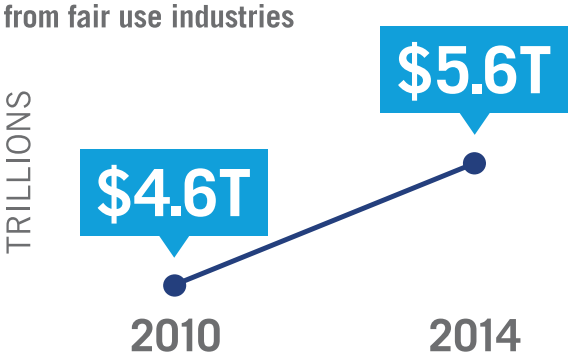
FAIR USE IN THE U.S. ECONOMY

2017 EDITION

Fair use industries have grown dramatically within the past 20 years, and their growth has had a profound impact on the U.S. economy in terms of revenue, value added to the U.S. economy, employment opportunities, and exports. Restrictions on fair use in the United States and unbalanced copyright policies abroad can endanger U.S. jobs, and economic growth and innovation.

REVENUE

from fair use industries



A $1.0 trillion expansion in four years

VALUE ADDED

2014 Data

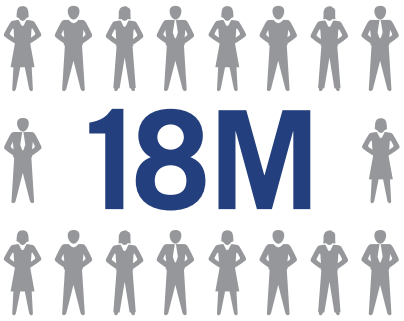
to U.S. economy

2.8T

Value added by fair use industries was $2.8 trillion, approximately 16 percent of total U.S. current dollar GDP

EMPLOYMENT

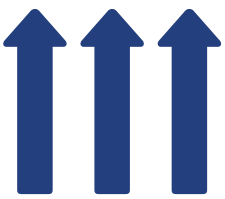
U.S. jobs in the fair use economy



18 million (about 1 in 8) U.S. workers benefit from fair use

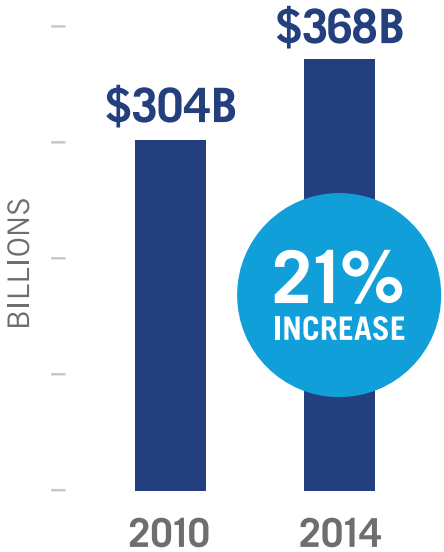
PRODUCTIVITY

3.2% annual increase in fair use industries from 2010 to 2014 (to about $155,000 per worker)



EXPORTS

of goods & services related to fair use industries



EXECUTIVE SUMMARY

In 2007, CCIA released a report prepared by Capital Trade, Inc. that was the first comprehensive study quantifying the U.S. economic contribution of industries relying on fair use and related legal provisions. The current report is the third update of the size and performance of the fair use economy. This study finds that in 2014, value added by fair use industries was 16 percent of the U.S. economy, employing 1 in 8 U.S. workers, and contributing $2.8 trillion to U.S. GDP. Meanwhile, the combined value added by industries that are the most reliant on fair use and other limitations and exceptions to copyright protections has more than tripled in size over 2002. From 2012 to 2014, the real output of these primary core industries accounted for 6.7 percent of real GDP growth, six times their current weight in the U.S. economy.

Findings

U.S. fair use industries:

- **Account for 16% of the U.S. economy**
- **Generate $5.6 trillion in annual revenue**
- **Employ 18 million U.S. workers, up 1 million over a 4-year period**
- **Increased annual productivity by 3.2%**
- **Increased U.S. exports by 21% over 4 years to $368 billion in 2014**

Understanding "Ancillary Copyright" in the Global Intellectual Property Environment

In recent years, some European governments have moved to impose a special levy on search engines and other online platforms providing the public with short fragments of news text, including quotations and headlines. This so-called "ancillary copyright" has been implemented in Germany and Spain, and traditional news publishers have called for similar rights in other countries.

This paper explores the nature and background of ancillary rights proposals, reviewing the jurisdictions in which rights in news and/or quotations have been extended thus far. It explains the background of ancillary rights, and discusses how these proposals violate existing international copyright law, as established by the Berne Convention, as well as trade laws and norms. The paper concludes that existing ancillary rights statutes could result in a valid claim before an international trade dispute resolution body.

1. The Birth of Ancillary Rights

Ancillary rights in news snippets and quotations are different from any existing intellectual property right. They are not patents, or trademarks, nor are they a form of industrial design or trade secret. Nor are ancillary rights equivalent to copyrights, since they create entitlements in content that international copyright law specifically declares to be ineligible for such protection. In this sense, they are *sui generis*. While couched in terms of an intellectual property right, ancillary rights are in fact an instrument of industrial policy. Aimed at rectifying perceived economic imbalances between industries, they act like a private tax or levy.[1] The purpose of these "snippet levies" is to compel one group of businesses—Internet businesses—to subsidize another group of businesses—news publishers.[2] International copyright law, however, does not regulate short phrases or facts, and it mandates that the right to quote not be abridged.[3]

This notion of a tax or levy on links or quotations (uses permitted under international law) is relatively new. The idea has been prompted by the well-documented difficulties of traditional print media in responding to and competing in the online environment. In the past few years certain European publishers' hostility to news aggregation and social media has grown, even though online services drive considerable traffic to the websites of news publishers, who then monetize that traffic by selling advertisements and/or subscriptions. To publishers who prefer that their content not be indexed or introduced to social media, long-standing protocols already provide highly granular control: news publishers can easily

[1] While ancillary copyright is frequently characterized as a tax (even by its supporters), the term 'tax' usually refers to monetary exactions imposed *and collected* by the state. Ancillary copyrights are monetary exactions imposed by the state but collected by a private actor. Thus, although the term 'tax' is accurate in a generic sense, ancillary copyrights may be more specifically characterized as a "levy."

[2] Ancillary rights are generally enforced by a "collective management entity," designated to act on behalf of news publishers and demand payment from regulated online platforms, aggregators and search providers.

[3] Berne Convention for the Protection of Literary and Artistic Works, art. 10(1), last revised July 24, 1971, amended Oct. 2, 1979, S. Treaty Doc. No. 99-27, 828 U.N.T.S. 221 (hereinafter "Berne Convention").

prevent that by complying with the robots.txt exclusion protocol, an Internet industry standard. By adding two short lines of code (containing fewer characters than this aside) in the header of a website, website administrators can prevent automated programs from copying headlines, snippets, or any other content from that site.

Some European news publishers, however, want it both ways. They want to maintain the high page-views and advertising rates associated with high search visibility, and they also want to be paid for the indexing necessary to send that traffic. They insist that online platforms must drive traffic to their sites, but also demand that online platforms pay for the "privilege" of being compelled to do so.

2. Nations Which Have Created "Rights" in Quotations or News Content

Germany

The first ancillary copyright statute was enacted in Germany. It resulted from demands by the German newspaper trade association BDZV[4] for payments from news aggregators in 2009. Opposition to the proposal within relevant governmental agencies, civil society groups, and academia kept legislation at bay for several years, until Germany's Federal Ministry of Justice ("*Bundesministerium der Justiz*") issued a draft proposal in July 2012 that would establish a new exclusive right for press publishers.[5] Germany enacted this proposal into its ancillary copyright law ("*Leistungsschutzrecht*") in August 2013.[6] This enactment upset the status quo under which search and social media platforms had the right to quote short excerpts from web content (as is the case with offline content), including content from newspapers, periodicals, and other press publishers.

This *Leistungsschutzrecht* expressly holds search engines liable for making available to the public parts of "press products" in search results, thereby creating direct liability for the automated indexing processes by which search results are generated. In a last minute change, however, the German legislature decided to exclude "smallest text excerpts" from the scope of the law. This created some legal uncertainty, as that term was given no definition. In theory, this phrase could include quotations and snippets, but such an interpretation might also be argued to render the provision largely irrelevant.

The law is specifically aimed at news aggregation.[7] It states that providing access to press publications remains permissible, as long as the access provider is not a commercial search service or similar entity.[8] The draft legislation's official background explanation clarified that this new restriction would not apply to "bloggers, other commercial businesses, associations, law firms or private and unpaid users."[9] In this manner, a German law firm (for example) might be permitted to compile links to news coverage on a particular topic, with accompanying snippets, without obtaining permission, but a search engine or social media provider would not. (If the hypothetical law firm were to use a social media provider to advertise its compilation, it remains unclear whether a remuneration obligation would accrue, and to whom.)

When in response to the *Leistungsschutzrecht* Google announced that it would de-index snippets from German publishers, the publishers' collecting society VG Media complained to German competition authorities. It took the position that Google was

[4] An acronym from the formal name, "Bundesverband Deutscher Zeitungsverleger e.V."

[5] Bundesministerium der Justiz, *Entwurf eines Siebenten Gesetzes zur Änderung des Urheberrechtsgesetzes* (July 7, 2012), art. 87g(4).

[6] German Copyright Act (1965, as last amended in 2013), at art. 87f(1), http://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html#p0572. Matt Schruers, *Germany Looks to Prop Up News Publishers With Snippet Subsidy, But Is a Quotation Tax Legal?*, Disruptive Competition Project (Nov. 14, 2012), http://www.project-disco.org/intellectual-property/111412-germany-looks-to-prop-up-news-publishers-with-snippet-subsidy-but-is-a-quotation-tax-legal.

[7] Jakob Kucharczyk, *Ancillary Copyright in Germany: From Opt-out to Opt-in on Google News*, Disruptive Competition Project (July 1, 2013), http://www.project-disco.org/intellectual-property/070113-ancillary-copyright-in-germany-from-opt-out-to-opt-in-on-google-news.

[8] See *supra* note 6, at art. 87g(4) (discussing "commercial providers of search engines or commercial providers of services which process the content accordingly").

[9] See *supra* note 5.

obligated to continue indexing its sites (and sending it traffic), and nevertheless still pay the levy.

The enactment of the law divided the German news publishing industry. While several major news outlets publicly refrained from exercising their right and explicitly allowed online aggregators to index their content, a second group of publishers gathered in the VG Media collecting society, which is trying to enforce the right for their members. In an interesting move, Axel Springer, one of Germany's biggest publishers and the most vocal supporter of the *Leistungsschutzrecht* at first insisted on enforcing the right, but ultimately granted a gratis license to Google only. Accordingly, the ancillary right has produced the inadvertent result of punishing smaller services.

CCIA and others have argued that this statute is inconsistent with Germany's international obligations.[10] In addition to representing a trade barrier, the statute has also been the subject of a challenge under German constitutional law, which remains pending.[11]

Spain

In Spain, the legislature introduced a similar snippet levy in 2014 in an omnibus reform of its *ley de propriedad intelectual* in July 2014.[12] Included within a broader reform known as the "canon AEDE,"[13] the snippet levy provision was enacted late in 2014, notwithstanding domestic criticism and substantive legal concerns. As enacted, Article 32.2 provides that:

> The making available to the public by electronic content aggregation service providers of non-significant fragments of aggregated content which are disclosed in periodic publications or on websites which are regularly updated, for the purposes of informing, shaping public opinion or entertaining, shall not require authorization, without prejudice to the publisher's right, or if appropriate, other right holders to receive equitable compensation. This right shall be unwaivable and will be given effect by means of intellectual property rights management entities...[14]

Depending upon whether quoted fragments are "significant" or "non-significant," regulated service providers appear to be obligated to obtain the publishers' permission to reproduce content, and provide "equitable compensation." If quoted fragments are "non-significant", regulated service providers need not obtain authorization to quote, but must still provide "equitable compensation."[15]

Spain's national competition enforcement authority ("CNMC") stated that a new exclusive right would form a barrier to market entry.[16] The CNMC further noted that the collecting society contemplated by the law might itself restrict competition, and recommended against a collecting society and also against creating an "unwaivable" right. Unlike its German counterpart, the Spanish legislation declares that the right is unwaivable, or inalienable. That is, news publishers cannot waive it and are prohibited from negotiating over the right to be remunerated; money must be paid for links whether it is desired by the content originator or not. This appears to include even cases

[10] *See generally* Comments of CCIA, Dkt. No. USTR-2012-0022, filed Feb. 8, 2013, http://www.ccianet.org/wp-content/uploads/library/CCIA%20Comments%20on%20Special%20301%20[2013].pdf (pointing out inconsistency of ancillary right proposal with international trade obligations in USTR's Special 301 proceeding).

[11] *See* Loek Essers, *German copyright law is unconstitutional, Yahoo says in complaint*, PCWorld (Aug. 1, 2014), http://www.pcworld.com/article/2460720/german-copyright-law-is-un-constitutional-yahoo-says-in-complaint.html (explaining Yahoo's claim that the law conflicts with the German constitutional protections to freedom of information and from government action restricting access to information).

[12] *See Boletín Oficial de las Cortes Generales, Congreso de los Diputados, Informe de la Ponencia: Proyecto de Ley por la que se modifica el Texto Refundido de la Ley de Propriedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil*, No. 81-3 (July 22, 2014), http://www.congreso.es/public_oficiales/L10/CONG/BOCG/A/BOCG-10-A-81-3.PDF.

[13] This informal label for the legislation is a reference the Spanish news publishers' trade organization, the Association of Spanish Editors and Newspapers (AEDE).

[14] *See supra* note 12. The revised Article 32.2 also curtails the right to reproduce images and photographic works that are disclosed in periodic publications or websites that are regularly updated. This provision is also problematic but is not addressed in this paper.

[15] While not explicitly stated in the legislation, this is implied by the provision's recognition of the "publisher's right, or if appropriate, other right holders to receive equitable compensation." The text indicates that the publisher's/right holder's right to equitable compensation applies at least in the case of non-significant fragments. Accordingly, it likely also applies in the case of significant fragments. It is unclear from the legislation whether there is an independent provision conferring this right directly.

[16] *See* Comisión Nacional de Los Mercados y La Competencia, "Proposal Relating to the Modification of Article 32.2 of the Draft Act Modifying the Redrafted Text of the Intellectual Property Act," (May 15, 2014), http://cnmcblog.es/wp-content/uploads/2014/05/140516-PRO_CNMC_0002_14-art-322PL.pdf.

where the author desires the content to be available under a more permissible basis, such as a Creative Commons license or open publishing. Like its German counterpart, the Spanish snippet levy purports to exclude non-commercial actors. Unlike Germany's law, however, the Spanish ancillary copyright could arguably be interpreted to cover just about any content online, not only news. This is because its scope includes content for "purposes of informing, shaping public opinion or entertaining" – a very broad definition of subject matter covered by the law.

The Spanish legislation went into effect on January 1, 2015, and contemplates creation of a collecting society or rights management organization, but as of the time of publication of this paper, no such entity yet existed. As a result of the law, Google exited the market for Spanish news aggregation, closing down its news.google.es website on December 16, 2014, and delisting links to Spanish news publications in Google search results.[17] Domestic online service providers like InfoAliment, a portal providing information related to the foods sector, have closed down their service as well.[18]

Other Jurisdictions

Similar proposals have also been aired in Austria, Italy, and Sweden, and in France with respect to images.[19] In addition, the European Commissioner for the Digital Economy and Society Günther Oettinger has called for an EU-wide measure, announcing in October 2014 that "[i]f Google uses and processes intellectual property from the EU, the EU can protect this property and can demand a charge."[20] However, it is currently uncertain whether an ancillary copyright provision will be part of a broader EU copyright law review.

It is noteworthy that under EU law, the Court of Justice of the EU (CJEU) stated in the 2014 *Svensson* holding that there is no copyright infringement when providing hyperlinks to freely accessible copyright-protected content.[21] That is because in such circumstances hyperlinks do not address a "new public" (*i.e.*, a public that was not taken into account by the rightholders when they authorized the initial communication). Insofar as ancillary copyrights negate the ability to link to freely accessible content online, they appear to conflict with this important right established by the CJEU in *Svensson*.

3. Quotation Rights Are Firmly Established in Many National Copyright Laws

U.S. law has historically denied copyright protection to facts[22] and titles,[23] while protecting the display of news snippets[24] and even lengthy quotations in news reporting.[25] The hostility to the protection of facts and news found in the U.S. legal system has also characterized the laws of many other countries—including European nations that are contemplating or have implemented ancillary rights provisions. As described in the Appendix, many countries' copyright

[17] Google Support, *Google Noticias en España*, https://support.google.com/news/answer/6140047#English.

[18] *InfoAliment.com Closes and Becomes First Victim of Google Tax*, Teinteresa (Dec. 11, 2014), http://www.teinteresa.es/tecno/Cierra-InfoAlimentcom-convierte-primera-Google_0_1264675766.html (translated from Spanish).

[19] Brad Spitz, *Thumbnails: French proposal for payment of royalties by search engines*, Kluwer Copyright Blog (Apr. 28, 2014), http://kluwercopyrightblog.com/2014/04/28/thumbnails-france/.

[20] *EU's Oettinger mulls levy on Google - Handelsblatt*, Reuters (Oct. 28, 2014), http://www.reuters.com/article/2014/10/28/eu-commission-oettinger-idUSL5N0SN34020141028; *Oettinger Floats Proposal for EU-wide 'Google-tax'*, EurActiv (Oct. 29, 2014), http://www.euractiv.com/sections/innovation-enterprise/oettinger-floats-proposal-eu-wide-google-tax-309568; *EU plant Urheberrechtsabgabe im Internet*, Handelsblatt (Oct. 28, 2014), http://www.handelsblatt.com/politik/international/schutz-geistigen-eigentums-bis-2016-eu-plant-urheberrechtsabgabe-im-internet/10900130.html ("...Wenn Google intellektuelle Werte aus der EU bezieht und damit arbeitet, dann kann die EU diese Werte schützen und von Google eine Abgabe dafür verlangen"). *See also* Frances Robinson & Tom Fairless, *EU Considers Taxing Google, Other U.S. Internet Firms*, Wall St. J. (Jan. 19, 2015), http://www.wsj.com/articles/eu-considers-taxing-google-other-u-s-internet-firms-1421699055. In a January 28 speech, Mr. Oettinger said a "Google 'levy' is an option" so that Internet platforms do not "hollow out" copyright. Video available *at* https://www.youtube.com/watch?v=jta92bxjMDw (original German, with English subtitles).

[21] Case C-466/12 *Svensson and Others*, Judgment of the Court of 13 Feb. 2014, http://curia.europa.eu/juris/liste.jsf?num=C-466/12.

[22] *See Feist Publ'ns, Inc. v. Rural Tele. Serv. Co., Inc.*, 499 U.S. 340, 344-45 (1991).

[23] 37 C.F.R. § 202.1(a). This remains true "[e]ven if a name, title, or short phrase is novel or distinctive." U.S. Copyright Office Circular 34, http://www.copyright.gov/circs/circ34.pdf. *See also Arnstein v. Porter*, 154 F.2d 464, 474 (2d Cir. 1946) ("A title cannot be copyrighted.").

[24] *See generally, e.g., Kelly v. Arriba Soft*, 336 F.3d 811 (9th Cir. 2003); *Perfect 10 v. Amazon.com*, 508 F. 3d 1146 (9th Cir. 2007); *Field v. Google*, 412 F. Supp. 2d 1106 (D. Nev. 2006).

[25] *See, e.g., Swatch Grp. Mgmt. v. Bloomberg LP*, 742 F.3d 17 (2d Cir. 2014) (news publication of entire transcript of analyst call does not infringe); *Fox Network News, LLC v. TVEyes, Inc.*, 2014 WL 4444043 (S.D.N.Y. Sept. 9, 2014).

laws contain firmly established prohibitions against copyright protection for facts. Laws throughout the developed world also provide explicit limitations and exceptions for news reporting, as well as quotation for various purposes. Developing countries also have provisions in their laws excluding protection of facts, and permitting quotation for news reporting and other purposes.[26]

4. Ancillary Rights and Similar "Snippet Taxes" Contravene International Obligations

The national laws discussed above arise from principles established in the earliest versions of the Berne Convention in 1886. Since its inception, Berne has guaranteed the right to quote from newspaper articles against newspaper copyright holders.[27]

> Article 10(1) of the Berne Convention provides:
>
> It *shall be* permissible to make quotations from a work which has already been lawfully made available to the public, provided that their making is compatible with fair practice, and their extent does not exceed that justified by the purpose, including quotations from newspaper articles and periodicals in the form of press summaries.[28]

Notably, the placement of "quotations" and "press summaries" after the provisos illustrates that these two items *cannot be limited* by the fair practice or 'exceeding the purpose' requirement. Rather, they are inherently exemplary of what satisfies these requirements. This interpretation is reaffirmed in the preparatory documents to the 1967 Stockholm Conference discussed further below. There, experts concluded after "exhaustive discussion" that these uses be included "by way of an example" of what was unambiguously permissible.

This interpretation also flows from the heading of Article 10, which refers to "*Free* Uses of Works". "Free," of course, is distinct from the "Permissible But Remunerated" uses contemplated by compulsory license schemes.[29] Consistent with this, the World Intellectual Property Organization characterized article 10(1) as permitting use "without the authorization of the owner of the copyright, and without payment of compensation."[30]

The negotiating history of the Berne Convention confirms this interpretation. In the first diplomatic conference on the Convention in the 1880s, the delegations referred to a "right" of quotation.[31] The history of the Berne Convention also illustrates that the quotation right should be interpreted broadly. Whereas prior to 1967 the right existed only to make "short quotations," the 1967 revision consciously deleted the word "short." This was not accidental; the change was specifically recommended by nations' international copyright experts. They reported:

> Sufficient direction in these various fields [referring to 'politics, economics, religion, and cultural life'] cannot be achieved unless it is possible to reproduce, in certain cases, fairly considerable portions of articles which constitute the contributions of other newspapers to public discussion.[32]

[26] *See* Appendix, *infra* (listing selected countries' copyright exceptions regarding permissibility of quotation, limited protection of news reporting, and non-protection of facts). *See also* Master List: Excerpts of Representative Copyright Limitations and Exceptions, http://infojustice.org/wp-content/uploads/2013/08/Masterlist-11262012.pdf, at 9-18.

[27] *See* Berne Convention (as of 1886), art. 7 (reprinted in 3 William F. Patry, Copyright Law & Practice Appx. F, at 1947 (1994 ed.)). The right originally authorized reproduction of entire articles.

[28] Berne Convention, art. 10(1) (emphasis supplied).

[29] *See, e.g.*, Sam Ricketson, *WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment*, WIPO Standing Committee on Copyright and Related Rights, SCCR/9/7 (Apr. 5, 2003) at 27 ("It is therefore clear that exceptions under Article 9(2) may take the form of either free uses or compulsory licenses, depending essentially on the number of reproductions made.").

[30] *See* WIPO, *Summary of the Berne Convention for the Protection of Literary and Artistic Works* (1886), http://www.wipo.int/treaties/en/ip/berne/summary_berne.html.

[31] *See, e.g.*, World Intell. Prop. Org., Berne Convention Centenary: 1886-1986, at 120 (1986) (referring to a "right" in an 1885 draft of the Convention to reproduce materials "excerpted from newspapers or periodical journals published in one of the countries of the union").

[32] World Intell. Prop. Org., 1 Records of the Intellectual Property Conference of Stockholm, June 11 to July 16, 1967, at 116 (1971).

The diplomatic conference minutes from 1967 reveal an unsuccessful French-Swiss proposal to re-insert the word "short" before "quotation." Diplomats considered and then overwhelmingly rejected the proposal, reaffirming the experts' recommendation that the quotation right should not be limited to "short" quotes.[33] The West German diplomat, one Mr. Reimer, said that his

> country could not support the proposal to inert the adjective "short" before the word quotations, because cases occurred in which quotations were permissible when they were not short; Article 51 of the Law which was in force in Germany was drafted on those lines and it placed no restriction on quotations in scientific or literary works, for instance, or on quotations from musical works. The Delegation of the Federal Republic of Germany thought it should be possible to delete the phrase "compatible with fair practice" or to replace it by some other phrase corresponding to the English term "fair use" or "fair dealing."[34]

These records demonstrate that the views of West Germany in 1967 – which were not openly contested at the time – were that quotations should not be restricted, and moreover, that the interpretation of "fair practice" should closely resemble fair dealing and fair use, which are *unremunerated*. This is consistent with WIPO's interpretation today that the phrase "*free* use" means without remuneration.[35]

Consistent with this conclusion, Berne art. 2(8) similarly states that its protection "shall not apply to news of the day or to miscellaneous facts having the character of mere items of press information." WIPO construed this limitation to mean that

> [t]he correct meaning of this provision is to exclude from protection articles containing news of the day or miscellaneous information, provided such articles have the character of simple press information, since news of this kind does not fulfil [sic] the conditions essential for admission to the category of literary or artistic works.[36]

More recently, UNESCO and WIPO collaborated on the development of a "model" law to aid nations in drafting copyright legislation that would comply with these international obligations: the Tunis Model Law on Copyright.[37] Article 7 of the Tunis instrument outlines "fair use" exceptions, including one for the quotation of news "without the author's consent."[38] (Several countries have already implemented very similar exceptions in their copyright statutes.[39])

In sum, German and Spanish laws, and similar efforts under consideration, upend established international copyright law. As noted above, most jurisdictions view displaying a short quotation or snippet to be permissible because: (a) it may be too short to qualify for copyright protection; (b) it may fall under an exception to copyright law – *e.g.*, because it is considered a fair practice, fair use, or fair dealing of the copyrighted work, including exceptions mandated by the Berne Convention; or (c) the copyright owner is considered to have granted its implied consent to showing such snippets (because it has made its work available on the Internet and is not blocking its work from being indexed by search engines).

[33] *Id*., vol. 2, at 860.

[34] *Id*.

[35] *See supra* note 30.

[36] *See supra* note 32, vol. 1, at 115.

[37] UNESCO & WIPO, *Tunis Model Law on Copyright* (1976), http://portal.unesco.org/culture/en/files/31318/11866635053tunis_model_law_en-web.pdf/tunis_model_law_en-web.pdf.

[38] Article 7(i)(b)("[T]he following uses of a protected work, either in the original language or in translation are permissible without the author's consent: [i]n the case of any work that has been lawfully published... the inclusion, subject to the mention of the source and the name of the author, of quotations from such work in another work, provided that such quotations are compatible with fair practice and their extent does not exceed that justified by the purpose, *including quotations form newspaper articles and periodicals in the form of press summaries*." (emphasis added)).

[39] *See generally* International Copyright Table, *infra* in Appendix.

5. Potential Trade Law Consequences of Ancillary Rights Statutes

Because established international copyright rules prohibit nations from restricting the right to quote, national legislation that contradicts these obligations breaches commitments made under the WTO.[40] This is because the provisions of Berne discussed here are incorporated in the Agreement on Trade-Related Aspects of Intellectual Property (TRIPS),[41] which is part of the WTO Agreement. Thus, WTO Members have a mandatory, affirmative obligation to permit anyone to quote from a work that is already lawfully publicly available.[42] An ancillary right or any other form of snippet tax would abrogate this right in violation of TRIPS obligations.

If there were any doubt that Berne obligations were enforceable under the WTO, that doubt was erased by a dispute brought by the European Union against the United States in 1999.[43] European rights-holders objected to Section 110(5) of the U.S. Copyright Act, which permits the public performance of music and television in certain public places (chiefly, small businesses, bars, and restaurants), without any royalty being paid. European trade authorities took up the complaint at the WTO, arguing that the provision violated Berne, and therefore TRIPS. While the U.S. Government argued that Section 110(5) was consistent with Berne, a WTO dispute resolution panel disagreed, and the United States agreed to pay $3.3 million to the European Union to seek to resolve the dispute.[44]

Ancillary rights are also difficult to reconcile with the market-opening objectives of the General Agreement on Trade in Services (GATS). For example, the EU committed not to limit market access, and to provide national treatment, to service suppliers of other WTO Members providing data processing services, advertising, and news and press agency services, including on a cross-border basis.[45] Imposing a levy upon service providers that applies disproportionately to foreign businesses may undermine these commitments.

6. Conclusion

Ancillary rights statutes contradict more than a century's worth of international copyright law, and disturb the harmony and balance within the international copyright system. By creating an independent government-granted right in content that is too short and often too insignificant to qualify for copyright protection, countries violate consensus, and more importantly, international trade law. Because the mandatory limitations of the Berne Convention are enforceable with trade law mechanisms, ancillary rights statutes should be challenged before the World Trade Organization, and elsewhere.

[40] *See* Raquel Xalabarder, *The Remunerated Statutory Limitation for News Aggregation and Search Engines Proposed by the Spanish Government - Its Compliance with International and EU Law*, IN3 Working Paper Series (Sept. 30, 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2504596.

[41] TRIPS Agreement, art. 9 ("Members shall comply with Articles 1 through 21 of the Berne Convention (1971)").

[42] This position has been advanced previously by CCIA in the USTR Special 301 process. *See, e.g.*, Comments of CCIA, Dkt. No. USTR-2010-003, filed Feb. 16, 2010, at 5, http://www.ccianet.org/wp-content/uploads/library/CCIA-2010-Spec301-cmts.pdf (if a Berne Contracting Party "were to prohibit the making of quotations from newspaper articles, for example, this would constitute denial of 'adequate and effective protection' under § 2242(a)(1), possibly necessitating identification as 'acts, policies, or practices' having actual or potential impact on relevant United States products."); *see also* Comments of CCIA, Dkt. No. USTR-2012-0022, filed Feb. 8, 2013, at 11-12, http://www.ccianet.org/wp-content/uploads/library/CCIA%20Comments%20on%20Special%20301%20[2013].pdf ("By virtue of Berne's incorporation in TRIPS, Article 10(1) imposes a mandatory, affirmative obligation on WTO Members to permit anyone to quote from a work that is already lawfully publicly available").

[43] *Panel Report, United States -- Section 110(5) of US Copyright Act*, WT/DS160/R, adopted July 27, 2000, ¶ 6.63 (finding not only that certain articles of the Berne Convention are incorporated into the TRIPS Agreement by way of Article 9.1, but also certain elements of the Berne Convention's *acquis*).

[44] Office of the U.S. Trade Representative, *Section 110(5) of US Copyright Act Dispute Settlement Proceeding Summary*, http://www.ustr.gov/trade-topics/enforcement/dispute-settlement-proceedings/united-states-%E2%80%94-section-1105-us-copyright-ac.

[45] *See Communication from the European Communities and its Member States*, WTO Doc. S/C/W/273, Oct. 9, 2006.

Appendix: Selected Countries' Copyright Exceptions Regarding Quotations, Facts, and News Reporting

The table below lists selected countries' copyright exceptions regarding permissibility of quotation, limited protection of news reporting, and non-protection of facts. This list is necessarily under-inclusive, since many common law countries' jurisprudence provides similar limitations which remain uncodified, such as the United States.[46]

Country	Statute	Article	Specific Language
Belgium	Law on Copyright and Neighboring Rights, http://www.wipo.int/edocs/lexdocs/laws/en/be/be064en.pdf	21	"Short quotations taken from a lawfully published work for the purpose of criticism... shall not infringe copyright."
Benin	Law No. 2005-30 of April 5, 2006 relating to Copyright and Related Rights of the Republic of Benin, http://www.wipo.int/edocs/lexdocs/laws/en/bj/bj002en.pdf	9	"The protection afforded by the present Law shall not extend to... the news of the day"
		15	"On condition that the title of the work and the name of its author are mentioned, analyses and short quotations from a work already lawfully made accessible to the public shall be lawful, provided that they are compatible with fair practice and insofar as they are justified by the intended scientific, critical, polemic, educational or informatory purpose, including quotations from newspaper articles and periodicals in the form of press summaries."
Brazil	Law No. 9610 of February 19, 1998, on Copyright and Neighboring Rights, http://www.wipo.int/edocs/lexdocs/laws/en/br/br002en.pdf	46(III)	"[T]he quotation in books, newspapers, magazines or any other medium of communication of passages from a work for the purposes of study, criticism or debate, to the extent justified by the purpose, provided that the author is named and the source of the quotation is given" is not a violation of copyright
China	Decision of the Standing Committee of the National People's Congress on Amending the Copyright Law of the People's Republic of China, http://www.wipo.int/edocs/lexdocs/laws/en/cn/cn031en.pdf	22	"Allow[ing] any 'appropriate' quotation from a published work in the context of one's own work. For a quotation to be appropriate, the quotation must be made solely for the purpose of introducing or commenting the quoted work in question for illustrating a point in one's own work."
		5(2)	"This law shall not be applicable to... news on current affairs."
Germany	Law on Copyright and Neighboring Rights, http://www.wipo.int/wipolex/en/text.jsp?file_id=126248	49	"It shall be permissible to reproduce and distribute individual broadcast commentaries and individual articles... from newspapers."
Greece	Law No. 2121/1993 on Copyright, Related Rights and Cultural Matters (as last amended by Law No. 3057/2002 (article 81) and by Law No. 3207/2003 (art. 10 par. 33), http://www.wipo.int/edocs/lexdocs/laws/en/gr/gr221en.pdf	2(5)	"The protection afforded under this Law [shall not apply] to expressions of folklore, news information or simple facts and data."
Hungary	Act No. LXXVI of 1999 on copyright, http://www.wipo.int/edocs/lexdocs/laws/en/hu/hu084en.pdf	1(5)	"Copyright protection shall not extend to facts and news items consisting of mere information serving as basis for press communications."

[46] *See, e.g., Feist Publ'ns, Inc. v. Rural Tele. Serv. Co., Inc.*, 499 U.S. 340, 344-45 (1991); *Fox Network News, LLC v. TVEyes, Inc.*, 2014 WL 4444043 (S.D.N.Y. Sept. 9, 2014).

Country	Statute	Article	Specific Language
India	Copyright Act, 1957 (as last amended by Act No. 49 of 1999), http://www.wipo.int/edocs/lexdocs/laws/en/in/in007en.pdf	52(1)(m)	"The reproduction in a newspaper, magazine or other periodical of an article on current economic, political, social or religious topics, unless the author of such article has expressly reserved to himself the right of such reproduction [is not infringement]."
Israel	Copyright Act of 2007, http://www.wipo.int/edocs/lexdocs/laws/en/il/il033en.pdf	5	"Copyright shall not extend to ideas,... facts or data, or news of the day."
Italy	Law No. 633 of April 22, 1941, for the Protection of Copyright and Neighboring Rights, http://www.wipo.int/wipolex/en/text.jsp?file_id=128286	65	"The reproduction or the communication to the public of works or protected subject-matters utilized during current events shall be permitted for the purposes of reporting the above current events and to the extent justified by the informatory purpose... "
		70	"The abridgment, quotation or reproduction of fragments or parts of a work and their communication to the public for the purpose of criticism or discussion, shall be permitted within the limits justified for such purposes, provided such acts do not conflict with the commercial exploitation of the work…"
Jordan	Law No. 22 of 1992 on Copyright and its Amendments up to 2005, http://www.wipo.int/edocs/lexdocs/laws/en/jo/jo070en.pdf	7(b)	"The protection stipulated under this law does not include the following products unless the groups of these products were characterized by a personal effort comprising innovation or order... [t]he published, broadcast or publicly notified news."
Korea	Copyright Act of 1957 (Act No. 432 of January 28, 1957, as amended up to Act No. 9625 of April 22, 2009), http://www.wipo.int/wipolex/en/text.jsp?file_id=190145	28	"It shall be permissible to make quotations from a work already made public: provided that they are within a reasonable limit for news reporting, criticism... and compatible with fair practices."
Malawi	Copyright Act of 1989, Law No. 9 April 26, 1989, http://www.wipo.int/edocs/lexdocs/laws/en/mw/mw004en.pdf	10(a)(ii)	"The following uses of a work under this Part, either in its original language or in its translation, shall be permissible without the author's consent and without the obligation to pay remuneration for the use of such work... in the case of any work that has been lawfully published... the inclusion, subject to mention of the source and the name of the author, of quotations from such work in another work, provided that such quotations are compatible with fair practice and their extent does not exceed that justified by the purpose, including quotations from newspaper articles and periodicals in the form of press summaries."
Malaysia	Copyright Act 1987 (Act 332, as of 1 January 2006), http://www.wipo.int/edocs/lexdocs/laws/en/my/my054en.pdf	13(2)(a), (m)	"[T]he right of control under that subsection does not include the right to control — the doing of any of the acts referred to in subsection (1) by way of fair dealing for purposes of non-profit research, private study, criticism, review or the reporting of current events, subject to the condition that if such use is public, it is accompanied by an acknowledgement of the title of the work and its authorship... [or] the making of quotations from a published work if they are compatible with fair practice and their extent does not exceed that justified by the purpose, including quotations from newspaper articles and periodicals in the form of press summaries: Provided that mention is made of the source and of the name of the author which appears on the work thus used."

Country	Statute	Article	Specific Language
Namibia	Copyright and Neighbouring Rights Protection Act, 1994 (Act No. 6 of 1994), http://www.wipo.int/edocs/lexdocs/laws/en/na/na002en.pdf	15(3)	"The copyright in a literary or musical work which is lawfully available to the public shall not be infringed by a quotation therefrom, including a quotation from an article in a newspaper, magazine or similar periodical that is in the form of a summary of that work, provided - (a) the quotation is compatible with fair practice; (b) the extent of the quotation does not exceed that justified by the purpose; and (c) the source and the name of the author, if that name appears on the work, are mentioned."
Norway	Copyright Act of 1961 (as of 1961), http://www.wipo.int/edocs/lexdocs/laws/en/no/no066en.pdf	22	"An issued work may be quoted, in accordance with proper usage and to the extent necessary to achieve the desired purpose."
Oman	Royal Decree No. 65/2008 promulgating the Law on Copyright and Related Rights, http://www.wipo.int/edocs/lexdocs/laws/en/om/om008en.pdf	4(b)	"Protection shall not cover mere ideas, procedures, working methods, mathematical concepts, principles, discoveries and data... [a]dditionally, protection shall not cover the following:... [n]ews of the day and current events which are mere journalistic information... [n]otwithstanding, all of the above in the previous paragraphs shall enjoy protection if their compilation or arrangement, or any creation or intellectual effort, eligible for protection, is distinguished."
Philippines	Intellectual Property Code of the Philippines (Republic Act No. 8293), http://www.wipo.int/edocs/lexdocs/laws/en/ph/ph001en.pdf	Chap VIII, §184.1(b)	"[T]he following acts shall not constitute infringement of copyright... he making of quotations from a published work if they are compatible with fair use and only to the extent justified for the purpose, including quotations from newspaper articles and periodicals in the form of press summaries: Provided, That the source and the name of the author, if appearing on the work, are mentioned."
Portugal	Code of Copyright and Related Rights (Law No. 45/85 of September 17, 1985, as last amended by Law No. 114/91 of September 3, 1991), http://www.wipo.int/edocs/lexdocs/laws/en/pt/pt002en.pdf	7	"The following may not be protected... news of the day and reports of events given simply for information, however disclosed."
South Africa	Copyright Act, 1978 (Act No. 98 of 1978, as amended up to Copyright Amendment Act 2002), http://www.wipo.int/edocs/lexdocs/laws/en/za/za002en.pdf	12	"The copyright in a literary or musical work which is lawfully available to the public shall not be infringed by any quotation therefrom, including any quotation from articles in newspapers or periodicals that are in the form of summaries of any such work: Provided that the quotation shall be compatible with fair practice, that the extent thereof shall not exceed the extent justified by the purpose and that the source shall be mentioned, as well as the name of the author if it appears on the work."
South Korea	Copyright Act of 1957 (Act No. 432 of January 28, 1957, as amended up to Act No. 5015 of December 6, 1995), http://www.wipo.int/edocs/lexdocs/laws/en/kr/kr001en.pdf	7(5) 25	"The following shall not be protected under this Act... [c]urrent news reports which transmit simple facts." "It shall be permissible to make quotations from a work already made public; provided that they are within a reasonable limit for news reporting, criticism, education and research, etc. and compatible with fair practice."
Sweden	Act on Copyright in Literary and Artistic Works (as of 1960), http://www.wipo.int/edocs/lexdocs/laws/en/se/se124en.pdf	22	"Anyone may, in accordance with proper usage and to the extent necessary for the purpose, quote from works which have been made available to the public."

Country	Statute	Article	Specific Language
Tunisia	Law No. 2009-33 of 23 June 2009 amending and supplementing Law No. 94 36 of 24 February 1994 on literary and artistic property, http://www.wipo.int/edocs/lexdocs/laws/en/tn/tn022en.pdf	Chap. II, Art. 11	"Quotations and borrowings from a work already lawfully made available to the public shall be authorized on condition that they are compatible with fair practice and are justified by a scientific, educational or informational purpose, including quotations and borrowings from articles in the form of press summaries. Such quotations and borrowings may be used in their original version or in translation and shall be accompanied by identification of the source and of the name of the author if his name is given in the source."
Turkey	Law No. 5846 of December 5, 1951 on Intellectual and Artistic Works (as last amended by Law No. 5728 of January 23, 2008), http://www.wipo.int/edocs/lexdocs/laws/en/tr/tr049en.pdf	36	"[D]aily news and information communicated to the public by the press or radio may be freely quoted. Articles or features on social, political or economic issues of the day published in newspapers or journals may be freely quoted in their original or adapted form in other newspapers or journals and may be broadcast by radio or disseminated by any other means, except where the right to quote them has been expressly reserved. Even where the right to quote is reserved, it is permitted to abridge such articles and features as a press review and to so quote, broadcast by radio or disseminate them in any other manner. In all such cases, mention must be made of the name, the issue and the date of the newspaper, of the journal, of the agency and of any other source from which the quotations have been made, together with the name, the pseudonym or the mark of the author of the articles"
Uganda	The Copyright and Neighbouring Rights Act, 2006, http://www.wipo.int/edocs/lexdocs/laws/en/ug/ug001en.pdf	7(d)	"The right to protection of copyrights under this Act shall not extend to the following works... news of the day namely reports of fresh events or current information by the media whether published in a written form, broadcast, internet or communicated to the public by any other means"
		15(1)(b)	"The fair use of a protected work in its original language or in a translation shall not be an infringement of the right of the author and shall not require the consent of the owner of the copyright where... a quotation from a published work is used in another work, including a quotation from a newspaper or periodical in the form of press summary, where — (i) the quotation is compatible with fair practice; and (ii) the extent of the quotation does not exceed what is justified for the purpose of the work in which the quotation is used, and (iii) acknowledgement is given to the work from which the quotation is made."
United Arab Emirates	Federal Law No. 40 of 1992 on the Protection of Intellectual Works and copyright, http://www.wipo.int/edocs/lexdocs/laws/en/ae/ae024en.pdf	6	"Protection prescribed in this law does not include the following items... [n]ews published, broadcasted or publicly announced."

Tech Policy Daily

Why "exporting" US copyright and communications law through trade agreements is a good idea

by: Markham Erickson, guest contributor, General Counsel to the Internet Association (http://www.techpolicydaily.com/author/markham-erickson/)
May 1, 2015 6:00 am

GlobalCopyrights by Shutterstock (http://www.shutterstock.com)

The United States is in the process of negotiating the Trans-Pacific Partnership (TPP), a new trade agreement aimed at boosting economic growth by providing meaningful market access for American goods and services abroad, and by setting clear rules for trade that protect the value of those exports. Congress is considering Trade Promotion Authority (TPA) legislation, which will serve as a statutory roadmap for our trade negotiators, providing detailed goals that Congress expects to be included in future agreements. The last time Congress amended the basic template of the TPA was 2002. It is high time that Congress update its guidance to the US Trade Representative (USTR), especially to reflect the central role the Internet now plays in innovation, economic growth, and democratic discourse.

The Internet economy comprises a significant portion of the global economy as a whole. In a five-year span, the Internet accounted for 21% of the GDP growth in mature economies (http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters), with 75% of the generated benefits captured by companies in more traditional industries. In the United States, the Internet accounted for 15% of GDP growth (http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters) over the same period of time. In 2006, e-commerce grew at more than twice the rate of the rest of the economy (http://www.ccianet.org/wp-content/uploads/library/Internet-Protectionism.pdf%20) and has continued to far-outpace (http://www.businessinsider.com/us-e-commerce-growth-is-now-far-outpacing-overall-retail-sales-2014-4) overall retail sales in the US. Since 2009, investment in Internet-specific businesses has doubled (https://apps.fcc.gov/edocs_public/attachmatch/DOC-326287A1.pdf) from $3.5 billion to over $7.1 billion. In 2013, Internet-focused firms including AT&T, Apple, Verizon, Comcast, and Google again ranked among the top 25 (http://www.progressivepolicy.org/wp-content/uploads/2014/10/2014.09-Carew_Mandel_US-Investment-Heroes-of-2014_Investing-at-Home-in-a-Connected-World.pdf) companies that made the most investments in the US economy for the year.

Internet companies in the United States have outpaced their worldwide competitors in no small part because the US has the most innovation-friendly legal system. The legal landscape against which our Internet economy has thrived was not achieved by accident. At the dawn of the commercial Internet, Congress enacted the Digital Millennium Copyright Act of 1998 (DMCA) and Section 230 of the Communications Decency Act, which ensure that Internet companies can innovate and grow without fear of liability for the actions of third parties who use the Internet to engage in unlawful activities. Twenty years before that, Congress codified fair use in Section 107 of the Copyright Act of 1976, which promotes innovation by providing limited exceptions to copyright restrictions. It is telling that the vast majority of countries around the world do not have any of these three statutes. Consequently, as our Internet companies increasingly become targets for protectionist initiatives in Europe and elsewhere, the US can no longer take for granted that our healthy, innovation-friendly legal system will become the standard around the globe.

That is why US Internet companies through their trade group, the Internet Association, have asked Congress to direct the USTR to include Section 230 and fair use-like principles in future trade agreements – contrary to the views recently expressed (http://www.techpolicydaily.com/technology/fair-use-tpp-bad-idea/) on TechPolicyDaily.com by AEI's Tom Sydnor.

Section 230 gives online service providers immunity from lawsuits brought against them based on content published by a third-party user of their services. Section 230 states in broad terms that "[n]o cause of action may be brought *and* no liability may be imposed under any State or local law that is inconsistent with this section." Section 230 applies to content posted on websites by third parties (such as defamatory statements). The protections of Section 230 are important because they encourage online commerce by providing uniformity and certainty for websites, web hosts, and online businesses that they will not be held liable for the unlawful activities of their users. Without Section 230, social media would not exist as we know it because Twitter, for example, would have to pre-screen every tweet prior to its posting – a task that the scale of the Internet makes impossible.

Fair use is an important part of copyright law that provides much-needed flexibility for both users and innovators. Copyright law is a strict liability regime that gives creators exclusive rights to control the publication and distribution of their works. Fair use provides a limited exception to those rights, which allows certain uses of works without first obtaining permission from the content creator. To understand the importance of fair use to today's innovation economy, consider that without fair use, technologies that we use every day and take for granted might never have been made availabl e. For example,

when you search for information on the Internet, you are not searching the World Wide Web but rather a copy of the World Wide Web that resides on the search engine's servers. Those copies are made without the permission of the website owners (who have a copyright in the creative content on the site), but this activity is lawful under fair use. A consumer that copies her music files from her laptop to smartphone does so pursuant to fair use. The basic functionalities of most digitally-enabled consumer electronic devices (*e.g.*, tablets, televisions, and DVRs) occur because of fair use. The list is nearly endless today and is only limited in the future by the creativity of the next Steve Jobs.

Imagine a legal regime that instead of fair use required a legislator or bureaucrat to specifically authorize a technology to function without running afoul of copyright protections. That is the reality in most of the world. Instead of an innovation-without-permission ecosystem, much of the world relies on the affirmative permission of governments before creating technologies that might violate copyright law. For example, civil-code countries enumerate uses of protected works that are permitted or excepted from copyright protections. Fortunately, USTR has taken an important first step in modernizing our trade agenda by embracing and promoting fair use-like principles in the TPP.

To the extent practicable, the balance of protections and exceptions provided by Section 230 and fair use together, as well as related policies, should be incorporated into future trade agreements.

Doing so will promote confidence and uniformity with our trading partners, provide legal certainty to one of the most important sectors to our economy, and assist our partners in the development of their own robust innovation economies. A modern trade agreement should incorporate the key drivers to today's economy. USTR has taken the first step. Congress should take the next by updating the TPA.

What the Five Year Anniversary of the SOPA/PIPA Blackout Can Teach Congress About Tech

from the *sopa,-pipa,-spotify-and-privacy* dept

Predictions
by Gary Shapiro
Thu, Jan 19th 2017
4:51pm

Five years ago this week, Americans opened their internet browsers and saw darkness.

Google, Wikipedia, Reddit, the Consumer Technology Association (CTA) and other major websites had banded together and gone dark to make a then-obscure piece of legislation infamous. Wikipedia shut down completely for 24 hours and a black band masked the Google logo.

These internet giants and other online sites joined millions of Americans in protesting the 2012 Stop Online Piracy Act (SOPA) and PROTECT IP Act (PIPA) legislation in a historic grassroots movement. More than four million people signed Google's online petition linked to the blacked-out homepage. Eight million people looked up **how to contact their representative** when **prompted to by Wikipedia**. Tumblr alone **produced 87,000 calls** to representatives. The vast numbers led most congressional sponsors to rescind their support of the bill.

SOPA and PIPA were well intended but ill-advised attempts on the part of Congress to protect the American copyright industry. But the legislation was so broad that it had the potential to harm or eradicate entire websites or online services, instead of specifically targeting individuals who uploaded illegal content.

The New York Times called the SOPA/PIPA protests a **"coming of age for the tech industry,"** and at CTA, we were proud to help lead this vital growth. It was a bipartisan and cross industry effort: venture capitalists and law professors, computer scientists and human rights advocates, progressives and tea partiers teamed together to fight the bills. Still, the bills progressed through Congress and appeared to have the momentum necessary to become law.

The 2012 CES proved to be one of the turning points. We **invited two legislators** — Republican Congressman Darrell Issa and Democratic Senator Ron Wyden — to Las Vegas to explain how the bill would jeopardize the freedom of the digital world. Both policymakers made strong, smart and passionate cases, and the press and attendees listened. Within days, the tide had reversed, and members of Congress ceased their support of the harmful bills. Weeks later, SOPA and PIPA were history.

We did this because we believe innovation, not an overbroad law, is the best way to grow the economy and fight piracy. History has proved us right. In five years since SOPA/PIPA failed, we've seen many instances of market disruptions and many more cases of technological innovation. Spotify, the now-ubiquitous Swedish streaming service, **intentionally developed** free streaming as a legal competitor to illegal piracy. It worked: **piracy has dropped significantly**. In 2013, less than 10 percent of daily web traffic in North America came from peer-to-peer file sharing compared to 31 percent in 2008.

Even more exciting, streaming services also led to significant revenue growth for the music industry. The Recording Industry Association of America, one of the major supporters of the SOPA/PIPA legislation, reported an **8.1 percent increase in overall revenues** from the first half of 2015 to the first half of 2016. This was due in large part to paid subscriptions to streaming services.

Other content industries have experienced massive growth as well. Video streaming programs such as Netflix, Amazon and Hulu **continue to thrive**. U.S. consumers spent 22 percent more on subscription video streaming services in 2016 than in 2015.

The combination of audio and video streaming takes up a whopping 71 percent of evening home entertainment in North America, and this number should only grow in the coming years. Once at odds on the floor of Congress, the innovation of the tech industry and the creativity of the media industries now mutually support and sustain one another's growth.

New technologies will lead to the same market disruptions that the internet prompted for the media industry. Will Congress support new technologies or stifle them? And how will legacy industries evolve to thrive in this changing technological landscape?

This year at CES 2017 in Las Vegas, innovators from around the globe came to exhibit technology that will change our world as we know it. Augmented and virtual reality technology will profoundly affect the media landscape, creating a more immersive and personalized experience. Drones have already changed the face of the retail industry, with Amazon making its first drone delivery in

time for the holiday season. Self-driving cars will revolutionize the auto industry, decrease traffic deaths and bring increased mobility to the elderly and those with disabilities. In dealing with the challenges that will inevitably arise, will Congress choose to preserve old models and technologies, or will it embrace the new and allow American ingenuity to lead?

Five years ago, members of Congress sided with progress over fear. The resulting explosion of innovation proved them right. As other new disruptive technologies emerge, we urge policymakers to heed the lessons of SOPA and PIPA and allow new innovations to prosper, thrive and move our society forward.

*Gary Shapiro is president and CEO of the Consumer Technology Association (CTA), the U.S. trade association representing more than 2,200 consumer technology companies, and author of the New York Times best-selling books, **Ninja Innovation: The Ten Killer Strategies of the World's Most Successful Businesses** and **The Comeback: How Innovation Will Restore the American Dream.** His views are his own. Connect with him on Twitter: **@GaryShapiro***

FREEDOM OF EXPRESSION

900 17th Street, N.W.
Suite 1100
Washington, DC 20006
Phone: 202.783.0070
Fax: 202.783.0534
Web: www.ccianet.org
Computer & Communications Industry Association

ABSTRACT

Internet Freedom: *How National Policies Have Failed To Protect It And What Can Be Done Now To Build It*

Executive Summary

Over the past decade the Internet has grown into the most efficient tool to spread information and knowledge around the world. The platform provides a level playing field for access to information and it gives disadvantaged people, underrepresented and oppressed groups around the world new opportunities to participate in economic, social, cultural and political activity.

Full access to the Internet and the ability to fully use it for communication and exchanging information, needs to be seen not just as a First Amendment issue in this country, but understood as a human rights issue around the world. Internet freedom is nothing less than freedom of expression in the 21st century.

Openness is inherent in the nature of the Internet, making it both effective and controversial. Totalitarian regimes have depended on tightly controlling the flow of information, both domestically and from the outside world, and they have been increasingly censoring the Internet to maintain their control of information.

Internet freedom has received attention this year as a full-fledged diplomatic issue. While spurred by recent headlines of Google's threat to leave China amid censorship and hacking concerns, the policy debate surrounding Internet freedom involve threats from many countries, which have been brewing for more than a decade.

Today's Internet suffers under the mismatch of a fully globalized technology infrastructure supported by piecemeal speech protection that varies from country to country. The problem grew from years of technological progress without any international framework accompanying that progress.

The lack of global consensus has allowed any foreign state to fill the vacuum with its own interpretation for how to manage this communications tool and to what extent traffic can be monitored, directed or controlled. For too long, Internet Access Providers and tech companies, rather than their governments, have been on the front lines of the battle for Internet openness in foreign countries.

As American Internet companies expand overseas, bringing with them our norms regarding openness and freedom of expression, they are often stymied by foreign rules. Other nations often apply their domestic laws in stifling or protectionist manners, obstructing U.S. businesses' access to markets, and impeding the free flow of information. The United States and other nations, which support freedom, must make clear to these governments that they oppose sabotaging what should be the greatest tool for advancing freedom, knowledge and commerce in the world.

Governments– not companies alone -- must primarily engage with other governments to combat policies that are antithetical to global Internet freedom. And while human rights and freedom of information remain highly visible and critical issues, it will likely take time even for democratic countries to agree on policies for Internet freedom and human rights. In the near term, the United States can start by setting a better example for Internet freedom with its own policies. Internet freedom and policies to ensure it should be a matter of negotiation in future international treaties or trade agreements. In the meantime, the US Trade Representative and State Department can

commit to enforcing existing trade laws, which already contain provisions that could help promote Internet freedom around the world.

Safeguarding the open flow of information and ideas over the Internet should rank at the top of our diplomatic agenda and trade agenda. Allowing Internet freedom to be eroded is one of the biggest omissions and failures of the past decade. But it's not too late to reverse this course and the Obama Administration seems to be paying attention.

WHY IS CENSORSHIP A TRADE ISSUE?

The United States is an information economy, and U.S. companies are leading vendors of information products and services. In this context, information discrimination fundamentally undermines market access for electronic commerce, and combating it should top our trade agenda.

.

- Information discrimination represents a classic "non-tariff trade barrier" (NTB) that we seek to eliminate when opening up foreign markets to U.S. goods. By co-opting U.S. businesses into content filtering, offenders create barriers to market entry that would not otherwise exist.

- Information discrimination constitutes an unfair "rule of origin" by filtering out (through a nontransparent process) U.S.-originating content, for example, certain U.S. domains that protectionist regimes deem to be "subversive."

- Information discrimination also violates the fundamental free trade principle of "national treatment" – it treats U.S. vendors differently by requiring U.S. companies to restrict access to information. Allowing U.S. companies to be perceived as being coerced into lowering their corporate moral standards leads to negative public reaction and even penalties at home.

INTERNET FREEDOM POLICY BREAKDOWNS:

Even as we denounce Internet censorship as too heavy-handed for a modern world, we must examine our own policies that impact Internet freedom. How is it possible that over the past decade we have not protected and advanced the values of open and free communications inherent in American culture and this American innovation? Seemingly small policy choices, which appear benign separately, add up to a national policy that itself may threaten Internet freedom.

1) International Policy Breakdowns

Until the recent actions by the Obama administration, the USTR and State Department failed to make Internet Freedom a human rights issue or a trade issue. Instead, U.S. policies presumed that more trade – even with compromises on censorship and related issues – would eventually lead to democratization. For years, the U.S. did not even raise censorship in the context of a trade concern until the Obama administration finally did last summer when China announced its Green Dam project to require all personal computers be sold with Internet filtering software.

- The USTR issued a report in February 2006 that purported to be a "top-to-bottom" review of U.S.-China trade relations, but did not mention the trade implications of coercing U.S. companies into censorship efforts. Instead the report focused on intellectual property rights infringement.
- The 2007 Country Reports on Human Rights Practices released in March 2008 by the State Department's Bureau of Democracy, Human Rights, and Labor downgraded China on its list of human rights abusers. China, which has been among the most vigorous in its Internet censorship, received a better report on human rights issues than the previous year even though the amount of

surveillance and censorship appeared to have increased.

- The Introduction of the 2008 Country Reports on Human Rights Practices does not mention Internet censorship in its section on developments in Vietnam. Reporters Without Borders ranks Vietnam on its list of Internet Enemies, citing a decree on Internet management and electronic communications that came into force in September 2008 forbidding opposition to the Socialist Republic of Vietnam.

- In May 2008, Iran's Committee in Charge of Determining Unauthorized Sites (CCDUS) expanded its blocking list to include many websites related to women's rights. The Introduction of the 2008 Country Reports on Human Rights Practices discusses women's rights and harassment and abuse of women's rights activists, but does not mention Internet censorship in its section on 2008 developments in Iran.

- Instead of helping tech and telecom companies combat demands of oppressive regimes, Congress responded with proposed legislation -- The Global Internet Freedom Act. GOFA would force U.S. Internet companies to exit nations such as China due to censorship and information demands, despite the positive impact the Internet has on expanding freedom in such countries.

2) Breakdowns In Internet Access Policies

The United States needs to lead by example, but we have not been doing so. Starting with some of the seemingly smaller, more innocuous changes to policy during the last administration, the FCC changed the status of Internet Access Providers and how they are regulated in ways that could pose a threat to Internet freedom and access.

- Internet access in the U.S. is controlled by a telecom (wireline+wireless) and cable duopoly, supplemented somewhat by less robust satellite services. The problems inherent in the lack of competition become evident when Internet Access Providers engage in censorship, as AT&T did when it censored certain anti-Bush lyrics performed by the musical band Pearl Jam on an AT&T webcast of the concert. Having few choices among IAPs also means consumers have little recourse when a company engages in improper filtering or censorship such as when lawful video file-sharing is blocked because it might compete with a cable IAP's own subscription programming.

- Phone companies during the past decade were successful in getting broadband connections classified as "information services"; no common carrier regulation has since been applied to Internet access. And access competition has flatlined. Thus, Americans have no exercisable right to affordable, open Internet access.

- Regulatory and court decisions from 2002-2005 eroded the clarity of legal protections from network level discrimination among end users and messages on the Internet. A content neutral Internet is what has made the Internet a level playing field for similar types of information to compete for attention. Net neutrality is a basic ingredient for freedom and openness of the Internet, but it has instead become a political debate, even in the United States.

- A year ago videos from an inaugural concert online were taken down after copyright violation complaints. Bloggers trying to comment on the presidential debates similarly faced fair use challenges when it came to sharing brief video clips of the debate on their websites.

3) Breakdowns In Policies Allowing Government To Access User Data

We understand there are appealing rationales for various types of censorship and surveillance, such as for security, but there is a cost to freedom nonetheless.

- Rather than deterring censorship, the government seeks greater Internet control for itself. The National Security Agency has allegedly engaged in warrantless wire-tapping of U.S.-based telephone calls.

- During the Bush administration, the Justice Department subpoenaed millions of search results from major U.S. search engines to help demonstrate that regulating sexually explicit Internet content can survive constitutional questions.

- Congress passed the USAPATRIOT Act, which expanded the ways government could obtain and monitor information online.

- Efforts by the executive branch and some in Congress to require long data retention policies clearly for the purpose of government searching private data.

- The federal government encouraged telecom companies to break the law and turn over information on customers without warrants in violation of federal communications law. It did so promising immunity and legal changes later in the Foreign Intelligence Surveillance Act. But such a practice undermines telecom and tech companies' ability to say 'no' to illegal requests of our government that infringe on customers – and make it even harder to refuse similar requests from foreign governments.

- The Washington Post reported Jan. 19, 2010, that the FBI accessed over 2000 phone records by filing requests citing what they later said were phony terrorism emergencies.

It is not that the United States' own electronic surveillance and monitoring initiatives are without some justification, though some are under judicial review. What matters is that such efforts are constitutionally suspect, especially when sweeping in scope, and they undercut U.S. companies' ability to resist heavy-handed regulation by foreign regimes. When being strong-armed by foreign governments U.S. Internet companies can hardly claim handing over user data contradicts American principles of free expression and privacy -- if they are being compelled to do so here.

Of course, warrantless monitoring of telephone calls, burdensome search engine subpoenas, and regulatory power grabs are not to be equated with the systematic oppression in authoritarian states. But quibbling about the order of magnitude of civilian monitoring isn't the sort of leadership that will backstop U.S. Internet companies when they are facing down the Thought Police whether in Beijing or elsewhere.

Moreover, to say that our government coerces Internet companies for noble causes while others do so to repress is missing the point: If our government chooses to lead the fight for Internet freedom, this would also provide political support to U.S. companies. Instead, our government's previous failure to lead, combined with its setting a bad example for the world, has pulled the rug out from companies, and has been a blow to Internet freedom.

If Internet Freedom is lost, it will be because it is the victim of well meaning efforts to address undesirable behavior on the Internet and half-hearted efforts to defend it.

U.S. POLICIES TO PROMOTE INTERNET FREEDOM

We don't want the government to write rules of Internet freedom, but ultimately to lay the groundwork for respecting openness and freedom as a value. To do so, our laws and policies must show leadership by example.

It will be an ongoing, but critical challenge for consumers, Internet-dependent businesses, citizens and our government to put overall Internet freedom ahead of various parochial interests in whatever policy debate of the day they manifest – net neutrality, IP protection, deep packet inspection, privacy, Internet surveillance or censorship. While these issues in Washington are often debated separately, they are all tied to a common ethic of Internet Freedom. We must support measures that promote this common ethic.

Domestic Policies:

- Carefully restrict the use of techniques such as deep packet inspection. Once set up, such practices could be used to do anything from going after alleged copyright infringement to monitoring and cracking down on political dissidents.

- Pass strong net neutrality rules so that no government entity here and no company may control access to the Internet. The US must join other nations in adopting best practices that promote Internet freedom and protecting the open Internet is one of them.

- Promote balanced IP law that does not restrict Internet access as a means of enforcing intellectual property rights.

- Block policy changes that would deputize Internet Access Providers to proactively investigate and enforce laws.

International Policies:

- Enhancing State Department and USTR Coordination: The State Department's Global Internet Freedom Task Force (GIFT) Strategy clearly states that the right to freedom of expression, provided for by both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, applies to communication on the Internet like other forms of communication. GIFT can raise awareness of Internet censorship, but there needs to be a coordinated effort across departments and agencies.

- The USTR must adopt a bolder approach to foreign roadblocks and respond forcefully to protectionist decisions abroad in countries like France instead of negotiating secret trade agreements like the Anti-Counterfeiting Trade Agreement (ACTA).

- Rather than rewarding governments whose courts punish U.S. businesses, we should advocate for common sense Internet laws overseas and focus on protecting the interests of U.S. Internet and e-commerce industries from foreign protectionism.

- We do not seek global governance as many would define it. We want commitment to not regulate the Internet, but simply ensure that access to it is open and not controlled by any country or company.

- The secrecy surrounding deliberations over ACTA threatens the open Internet by perpetuating a norm that secret Internet regulation is acceptable. The policy of ACTA secrecy should be repudiated and discussions about Internet regulation should occur in open, multilateral forums.

- To achieve a minimum level of parity, United States trading partners must provide Internet services safe harbors for user-generated content, permit the use of online materials in relation to providing search functionality, and allow de minimis, nominative uses of trademarks.

- A newly networked world demands a new understanding of trade barriers. There must be a framework to address the issue of free flow of information. This profound issue must be championed primarily on the governmental level, rather than by industry. It must also be addressed multilaterally and bilaterally. The successful result on Green Dam was due in part to the coordination between the U.S. and allies like the E.U. and Japan. Our government and others committed to the free flow of information need to come up with rules of the road for this new, networked world, perhaps through an International Internet Freedom Agreement.

CONCLUSION

U.S. officials and human rights activists around the world have shown a growing understanding of the power of the Internet to be either the greatest tool for freedom of speech and participation in a democracy, or the most efficient tool ever to repress speech and maintain a closed society.

The battle is larger than headlines like the showdown between a search engine and the Chinese government. Recent events, however, should be a wake up call to fight for Internet freedom – for protecting that openness and access for citizens around the world. As we consider various domestic and international policies, attention should be paid to whether they support or diminish Internet freedom. Perhaps the greatest threat to Internet freedom is death by a thousand cuts – not a sudden fatal blow, but a chipping away of the openness as everyone from the federal government to local sheriffs ask to monitor or surveil Internet users.

If the Internet is to fulfill its potential as the printing press of the Digital Age, neither a government nor an IAP should act as a gatekeeper, quashing access at its whim. Governments that censor may not easily change their ways, but they need to be made to understand the depth of the U.S. commitment to Internet freedom. We must elevate this issue to the top of our diplomatic and trade agendas, thereby helping other nations understand our commitment to curbing threats to Internet freedom in whatever form they manifest.

PRIVACY AND SECURITY

Privacy

Information Technology Industry Council

Global Principles for Governments Collecting Private Sector Data from Commercial Entities

Recognizing that governments around the world engage in surveillance activities; and

Recognizing that certain important considerations must be built into government access to private sector data in the course of surveillance activities;

The principles below are intended to apply to government collection of private sector data from commercial entities.

I. **Lawful Basis and Necessity**. Any government collection of private sector data must be authorized by law, must not be indiscriminate, and must be limited to what is necessary to achieve a legitimate purpose. Laws that authorize government collection of such data should include: (a) appropriate procedural protections under certain circumstances; and (b) sunset provisions to ensure regular reviews to determine whether specific laws continue to be necessary, or need to be amended.

II. **Access**. Access to private sector data collected by governments from commercial entities should be restricted to only those within government who need such access consistent with the intended purpose of such collection or as authorized by law.

III. **Technology Neutrality**. The limitations on government data collection, and the procedural legal requirements that governments must adhere to in connection with such collection, should apply equally to all types of data, including both offline and online data, and across technologies and platforms.

IV. **Transparency**. Governments should implement appropriate transparency measures about the programs and mechanisms utilized to collect private sector data. Commercial entities should be permitted to disclose certain appropriate information about the government requests they receive for private sector data.

V. **Oversight**. Programs and mechanisms pursuant to which a government collects private sector data should be subject to meaningful oversight by an independent body established by the government. Such independent body should have sufficient powers to access relevant information to assess whether there is a legal basis for how the government conducts its private sector data collection activities and to make appropriate policy recommendations.

VI. **Avoid Conflict of Laws**. Governments should: (a) recognize that global commercial entities may be subject to the laws of numerous jurisdictions with respect to the collection of private sector data by governments; and (b) endeavor to avoid conflicts among such laws.

VII. **International Engagement**. Governments should recognize that the frameworks pursuant to which national governments collect private sector data have global impacts. Governments should engage in multilateral discussions with other governments to minimize adverse global impacts in connection with the collection of such data.

Reform Government Surveillance Letter to House and Senate Leadership: Lawful Access Priorities for 2017

Dear Leader McConnell, Speaker Ryan, Minority Leader Schumer and Minority Leader Pelosi:

The Reform Government Surveillance coalition (RGS) writes to share with you our priorities for this Congress with regard to reforming laws that govern when law enforcement and the intelligence community may access user data. As you shape Congress' agenda, we look forward to working with you on important legislation that has an impact on the information of billions of our customers around the globe.

Our customers, both individual and corporate, no matter where they are located, expect us to protect the privacy and security of their data. At the same time, law enforcement officials should have the resources that they need to better protect our communities. As a result, we have adopted the following principles that we believe must define government surveillance laws in the U.S. and throughout the world:

Limiting Governments' Authority to Collect Users' Information - Governments should codify sensible limitations on their ability to compel service providers to disclose user data

that balance their need for the data in limited circumstances, users' reasonable privacy interests, and the impact on trust in the Internet. In addition, governments should limit surveillance to specific, known uses for lawful purposes, and should not undertake bulk data collection of Internet communications.

Oversight and Accountability - Intelligence agencies seeking to collect or compel the production of information should do so under a clear legal framework in which executive powers are subject to strong checks and balances. Reviewing courts should be independent and include an adversarial process, and governments should allow important rulings of law to be made public in a timely manner so that the courts are accountable to an informed citizenry.

Transparency About Government Demands - Transparency is essential to a debate over governments' surveillance powers and the scope of programs that are administered under those powers. Governments should allow companies to publish the number and nature of government demands for user information. In addition, governments should also promptly and publicly disclose this data.

Respecting the Free Flow of Information - The ability of data to flow or be accessed across borders is essential to a robust 21st century global economy. Governments should permit the transfer of data and should not inhibit access by companies or individuals to lawfully available information that is stored outside of the country. Governments should not require service providers to locate infrastructure within a country's borders or to operate locally.

Avoiding Conflicts Among Governments - In order to avoid conflicting laws, there should be a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions, such as improved Mutual Legal Assistance Treaty — or "MLAT" — processes. Where the laws of one jurisdiction conflict with the laws of another, it is incumbent upon governments to work together to resolve the conflict.

Adopting policies that adhere to these principles is important for fostering our shared commitment to the privacy and security of our customers and their data, and for preserving the health of the Internet economy. Accordingly, the following legislative proposals are on RGS' agenda for this Congress:

(1) **Passage of the Email Privacy Act:** As we have in the past, RGS companies strongly support passage of the Email Privacy Act. The Electronic Communications Privacy Act (ECPA), which it would amend, was passed when email was virtually unheard of (and used almost exclusively by businesses) and "mobile" content on cell phones and tablets did not exist. We applaud the passage of the unanimously supported Email Privacy Act by the House of Representatives, and we look forward to continuing to work on reforming ECPA, including with respect to ECPA's current regime for secrecy orders. When secrecy around a government warrant is needed, orders that require email providers to keep these types of legal demands secret should be the exception and not the rule.

(2) **A rights-protecting regime for when law enforcement asks for data across borders:** Governments all over the world are adopting the position that they can request a suspect's data regardless of the conflicts of law or international norms and treaties. This new reality is weakening trust in technology among business and consumers and is incentivizing foreign governments to consider data localization laws and other policies that would fragment the Internet and impede the flow of data and commerce across borders. At the same time, law enforcement needs mechanisms to lawfully obtain data for investigations and to protect their citizens. The MLAT process remains an important tool for this and should be modernized, but a complementary process is needed to respond to the increased number of requests for cross-border requests for digital information.

Last year, the Department of Justice sent to the House and Senate Judiciary Committees language that would enable law enforcement in another country to issue legal process for

content data held by U.S. companies. A country could only issue legal process directly to U.S. companies if it enters into an agreement with the United States that requires the requests that are issued by a foreign country to meet strong standards of transparency, oversight, and due process. RGS supports legislation like this as long as it protects human rights and privacy rights (set forth in more detail here), and looks forward to working with policymakers and stakeholders on the introduction and passage of a bill that would meet these criteria.

(3) **Addressing the global nature of data under ECPA:** Last year, the United States Court of Appeal for the Second Circuit held that ECPA is not extraterritorial in its reach; in other words, a warrant issued under ECPA cannot be used to obtain data from a US company where that data is not stored in the US. (Since then, a court in the Eastern District of Pennsylvania has held that ECPA warrants can be used to compel the production of user data stored abroad.) In order to protect the privacy of customers both in the US and worldwide, and to ensure that law enforcement can get the information that it needs pursuant to a lawful order, the International Communications Privacy Act was introduced last year by Senators Hatch, Coons, and Heller in the Senate and Representatives Marino and DelBene in the House. RGS supports the passage of ICPA and welcomes discussion about any other approaches to this issue that are workable from a technological perspective, protective of consumers' privacy and due process rights, and able to meet the needs of law enforcement.

(4) **Reforming the expiring powers of Section 702 of the FISA Amendments Act of 2008:** Section 702 of the FISA Amendments Act expires at the end of 2017. RGS would like to work with you, law enforcement, the intelligence community, civil liberties and privacy groups, and any other stakeholder to help improve oversight of and transparency of this authority.

Section 702 provides the legal underpinnings and judicial supervision for intelligence-gathering programs used by our intelligence community. As Congress moves

towards reauthorizing these powers, we would support changes to Section 702 that enhance transparency, provide greater programmatic oversight, and strengthen protection of sensitive personal data. Among the reforms that we would like to work with you on are narrowing the type of information that can be collected under Section 702; requiring judicial oversight for searching the contents of 702 material for the communications of a US person (given that US persons are not the target of 702); allowing companies to disclose the number of requests they receive by legal authority; further declassification of FISA Court orders; and providing greater transparency around how the communications of US persons that are incidentally collected under Section 702 are searched and used, including how often it is "queried" using identifiers that are tied to US persons.

We look forward to working with you to help ensure that an appropriate balance is struck between the government's need for critical information and people's privacy and due process rights.

Thank you very much, as always, for your hard work on these issues that are of central importance to our government and our economy.

Signed,

Reform Government Surveillance

cc:
The Honorable Bob Goodlatte, Chairman, House Judiciary Committee
The Honorable John Conyers, Ranking Member, House Judiciary Committee
The Honorable Devin Nunes, Chairman, House Intelligence Committee
The Honorable Adam Schiff, Ranking Member, House Intelligence Committee
The Honorable Chuck Grassley, Chairman, Senate Judiciary Committee
The Honorable Dianne Feinstein, Ranking Member, Senate Judiciary Committee
The Honorable Richard Burr, Chairman, Senate Intelligence Committee
The Honorable Mark Warner, Vice Chairman, Senate Intelligence Committee

Feb 28th, 2017

PRIVACY AND SECURITY

Encryption

BLAST FROM THE PAST: LEARNING LESSONS FROM PREVIOUS PANICS OVER UBIQUITOUS STRONG ENCRYPTION

by BIJAN MADHANI *on* SEPTEMBER 10, 2015

Over the past several months, the tech industry has been experiencing a terrible bout of déjà vu. In a campaign led by FBI Director James Comey, law enforcement and intelligence community voices have argued against the proliferation of ubiquitous strong encryption in consumer devices and communication platforms. By ubiquitous strong encryption, I mean both the expanded availability of device encryption for smartphones, and end-to-end encryption of communications protocols with only the sender and recipient (but no third parties) holding keys.

This sort of strong encryption has proliferated for a variety of reasons. Hacks and data breaches are larger, more consequential, and more prevalent than ever. The last two years have also been marked by controversy over widespread government surveillance in the U.S. and elsewhere. These circumstances have caused consumers to demand, and technology companies to develop, the tools to protect sensitive personal and financial information from those who consumers would prefer not have access.

Naturally, the renewed focus on product and platform security on behalf of consumers has led to conflict between the tech industry and law enforcement. Governments fear "going dark"—the idea that there will be some set of encrypted communications and content that they will not be able to access even after having obtained the necessary legal process to seek that information, which in the U.S. usually means a search warrant.

If "going dark" sounds somewhat familiar, that's because these are largely the same fears that led to the first "Crypto Wars" in the United States.

By the early 1990s, researchers had begun developing the first widely available strong encryption tools, including protocols like PGP. In response, the Clinton Administration pushed to limit the export of higher-grade encryption protocols. As a result, a class of "export-grade" encryption was developed for use in

countries where the export strong encryption was prohibited. Some "key escrow" solutions were also developed for commercial use, like the Clipper Chip, which would allow the government or a trusted third party to hold the master keys to decrypt communications sent via devices using the protocols on that chip. Ultimately, once privacy advocates, industry, and technologists joined together in opposition (and after technical flaws were found in the Clipper Chip specification), the government largely backed down from its opposition to products containing strong encryption.

Winning that fight and enabling the use of secure protocols in electronic communication and transaction systems helped build public trust in the Internet, something that users continue to value. Without the underlying confidence in the integrity and security of the Internet and associated applications, it would not have developed into the successful platform for digital speech and commerce that it is today.

What the FBI and others are looking for now is essentially the same as what the government sought in the 1990s. All the same arguments, both in law enforcement's favor and against it, apply today. Whether consumers are allowed to use widely available strong encryption on their personal devices and take advantage of communications services that employ it end-to-end remains a cost-benefit problem informed by technical and Constitutional limits.

Technical Limitations

> *"The deployment of key-recovery-based encryption infrastructures to meet law enforcement's stated specifications will result in substantial sacrifices in security and greatly increased costs to the end user. Building the secure computer-communication infrastructures necessary to provide adequate technological underpinnings demanded by these requirements would be enormously complex and is far beyond the experience and current competency of the field.*

The above quote is from a technical report produced by eleven preeminent computer scientists. In it they analyzed some of the key escrow encryption requirements suggested by government agencies. The report is from 1997.

The government contends that given technical progress in the intervening years and a little good ol' fashioned American ingenuity, technology companies should be able to develop and implement a key escrow or split-key or "golden" key protocol that makes all parties happy without sacrificing security. Optimism aside, the technical limitations of a key escrow solution have not changed since '97. A report prepared this year by another group of computer security experts makes largely the same arguments as presented in the 1997 report:

- Digital devices and communications tools are extremely complex systems, and complexity is the enemy of security. Devising an additional layer of complexity at scale to permit third-party access to encrypted consumer devices and communications will likely create new vulnerabilities or exacerbate existing ones.
- Current encryption protocols are also designed to improve security through forward secrecy—"where decryption keys are deleted immediately after use, so that stealing the encryption key used by a communications server would not compromise earlier or later communications."
- Key escrow solutions require some third party—be it the provider, law enforcement, or some other entity—to retain security credentials for later use by the government. That third party would

immediately become a rich target for hackers of all stripes.

Split key-solutions, where multiple parties hold a decryption key, can reduce the risk associated with the a single third party holding credentials and becoming a target. However, they further increase the complexity of technical systems, and do nothing to reduce the substantial aggregate economic and societal costs detailed below.

The Fourth Amendment

While technical arguments against weakening strong encryption seemingly hold no water for the starry-eyed dreamers at the FBI, the Constitution certainly should. The Fourth Amendment preserves the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and requires probable cause before the issuance of any warrants. It explicitly protects "a right of the people." However, the law enforcement interests working against strong encryption would have the public believe that the Fourth Amendment should be read in the inverse. It is true that the FBI and other U.S. law enforcement agencies argue that they only wish to decrypt encrypted communications after obtaining a warrant based on probable cause. But having a search warrant doesn't mean that the government then has a positive right of its own to exercise—its agents merely have authorization from a court to intrude upon the privacy of a specific person and search for a particular thing they wish to seize. Yet the FBI seemingly believes that in the digital world, a search warrant is in fact a right to whatever means or assistance that they deem necessary to access the personal effects they seek.

There's a reason the legal process the FBI seeks from federal judges is called a search warrant, and not a "find warrant." In the physical world, when law enforcement officers execute a search warrant, the person whose home is being searched does not have to unlock every safe or locked room at the government's instruction, nor does he have to lead the officers to every particular piece of evidence that they seek. And if the government's agents encounter a safe that they cannot crack, they do not require that the manufacturer ensure that future products be designed in a manner accessible to law enforcement when they have warrants.

The rules should be no different with respect to digital communications and electronic devices. When law enforcement obtains a probable cause-based search warrant for particular content in an individual's smartphone or electronic messages, they have authorization from a court to acquire that smartphone if they can find it, and access those messages in whatever form they are stored. In the event the smartphone or messages sought are encrypted, the government can use legal tools to compel the owner to give them access. But, like the safe maker who does not design his products to the specifications of law enforcement needs, third party device manufacturers and communications providers should not have to design their technologies according to the requirements of law enforcement agents who may at some point have warrants.

Building or retrofitting encryption systems to enable easy access for the government through a key escrow or split key mechanism flies in the face of the motivations underlying the Fourth Amendment. The general principle of the Fourth Amendment is that it serves as a check on government activities, not a license, and limited ability to search afforded to the government by the issuance of a search warrant should not swallow that rule in either the physical or digital context.

Weighing Costs and Benefits

The FBI's position is not without some merit. The fear of "going dark" is a result of a few cases where federal and state law enforcement have encountered difficulty in investigating crimes because devices have been encrypted in a manner that agents were not able to successfully circumvent. For the FBI, it follows that as strong encryption grows more readily available, the number of serious crimes that they cannot solve will increase correspondingly, accompanied by an increase in the potential terrorists that might not be discovered.

Of course, the government can only count a handful of cases that have been recently stymied in some way by the presence of encryption, and none that went unsolved as a result. As for truly committed bad actors like potential terrorists, limiting the availability or effectiveness of encryption available through American services and devices will only drive them to less law-abiding providers in less hospitable reaches of the Internet and globe.

The few benefits of limiting strong encryption are likely outweighed by the aggregate costs. As reports produced by computer security experts detail, developing and implementing encryption systems that incorporate mechanisms through which third parties can access and decrypt secured communications and content is complicated and will introduce vulnerabilities. Some of those vulnerabilities are obvious, like the existence of some entity that must hold cryptographic keys in escrow. These sorts of entities are rich targets for hackers, and prominent firms have already been breached and had their keys compromised.

Other vulnerabilities are less evident, and may only become apparent years down the line, as a result of the complexity of supporting and implementing encryption protocols that satisfy government needs. For example, just this spring, an attack known as Logjam exploited residual application support of weak export-grade cryptography. That was the same export-grade cryptography developed in the 1990s to meet then-existing government restrictions on the distribution of strong encryption. The Logjam vulnerability took two decades to discover. Today, encryption is relied upon and embedded in systems to a much greater degree for commerce and communication, and as a result, vulnerabilities will propagate at a much higher rate, with a much lower likelihood of discovery.

Law enforcement and the intelligence community are not the only government agencies with an interest in the adoption of encryption. The FTC has long cited the use of encryption as a best practice to protect consumers and avoid violation of Section 5 of the FTC Act. The current Chief Technology Officer of the FTC recently advocated for consumers' use of full disk encryption on their personal devices. And even the FBI, until its current about-face, encouraged users of smartphones to use OS encryption to protect their devices from thieves. The FTC and divisions of the FBI tasked with dealing with the consumer protection and criminal implications of increased fraud and identity theft recognize the steadily growing economic and personal costs of data breaches. They also know through experience that without widespread use of encryption, the already significant aggregate impacts of hacks would be exacerbated.

Requiring a split key or key escrow system for U.S. providers and manufacturers to allow access to the U.S. government would have far reaching outcomes internationally as well. The adoption of a government-access regime for encryption in the U.S. would likely also be used as a license for other countries, particularly those less enamored by the rule of law, to do the same. Not being able to communicate securely would have a chilling effect on the the speech of dissidents and journalists worldwide. In addition, the international competitiveness of the U.S. tech industry has already been harmed by disclosures of mass surveillance by the U.S. intelligence community. This trust deficit would only be deepened by the news that U.S. companies have

designed systems to allow the U.S. government to better access the contents of encrypted devices and messages, which would simply lead to more customers lost to international competitors.

Talking in Code

The FBI has repeatedly stated that it seeks, first and foremost, a public conversation on what law enforcement views as a significant looming hindrance to its investigatory capabilities. The goal of this public conversation is for American society to decide (yet again) whether it prefers the costs and benefits of ubiquitous strong encryption or those associated with weakened or less-available encryption tools. It's worth noting that a former NSA Director, Secretary of Homeland Security, and Deputy Secretary of Defense recently contributed their thoughts to the conversation, and have come down on the side of strong encryption, largely for the reasons listed above.

The government asks whether tech companies are willing to abide by the public's will if it decides that the risks of going dark are too great. That's the wrong question, because the public made its decision loud and clear in the first Crypto Wars and again in demanding the development of better security measures for their devices and communications. So perhaps the better question to ask is when the government is going to listen.

Issue brief: A "backdoor" to encryption for government surveillance

Encrypting smartphones and other devices helps protect against malicious hacking, identity theft, phone theft, and other crimes. However, a government mandate requiring companies to build a "backdoor" into encryption for surveillance would put consumers at grave risk and impose heavy costs on US businesses. The government can obtain information for investigations from other sources, and may be able to compel an individual to decrypt information with a search warrant.

What companies have done recently: Apple and Google recently announced that their smartphones will be "encrypted by default."[1] All the data stored on the phone itself will be unreadable to anyone who accesses the phone without knowing the device passcode, in order to unlock the encryption. Weak encryption (or obvious passwords) can be broken, but Apple and Google will apply strong encryption to their devices.[2] Many other companies and nonprofits have long offered products and services secured by strong encryption to the public.[3]

> **The primary impact:** Mobile devices increasingly mediate the most sensitive of our online transactions, from health to finance to authenticating to secure systems. Encrypting mobile devices by default will increase security from cybercriminals for regular smartphone users. Encryption by default ensures that if criminals steal or attempt to hack into a phone, they will be unable to access the owner's sensitive data on the device, such as credit card information, photos, emails, medical records, social media accounts, and authentication credentials.[4] The principle objective of securing smartphones with strong encryption is to protect against cybersecurity threats faced by millions of American smartphone users – identity theft, phone theft, and cybercrime.[5]

What the FBI wants: The FBI wants a "backdoor" into encrypted products – not just phones, but other communications services as well. FBI Director Comey has called for companies to build security flaws into their encrypted products so that the government can break through and wiretap consumers or seize data stored on their devices.[6] In the case of the San Bernardino shooting, the FBI has sought to force Apple, Inc. to produce an insecure version of its mobile operating system, which would vastly increase the security and privacy risks to hundreds of millions mobile devices.

> **A backdoor for government surveillance:** Director Comey has stated the FBI is not seeking a backdoor because he is proposing that companies intentionally build into their products a means of breaking encryption for the purpose of government access. However, this conflates a legal backdoor with a technical one: as a technical matter, creating a path through encryption to provide access that the user does not authorize is, by definition, a "backdoor" security vulnerability. It is impossible to build encryption that can be circumvented without creating a technical backdoor.

Backdoors create major problems: Backdoors severely weaken cybersecurity, leaving users exposed to malicious hacking and crime. A government-mandated security vulnerability in tech products would also be a huge burden on businesses and an obstacle to innovation.

> **User security undermined:** A fundamental problem with a backdoor is that there is no way to control who goes through it.[7] If the US government can exploit a backdoor security vulnerability to access a consumer's device, so will malicious hackers, identity thieves, and foreign governments.[8] This will devastate the security of not just individual consumers around the world, but also the many businesses that use American commercial tech products day-to-day. Ultimately, this mandate would have the effect of actually enabling cybercrime and undermining national security.

---

[1] Joe Miller, Google and Apple to introduce default encryption, BBC News, Sep. 19, 2014, http://www.bbc.com/news/technology-29276955.
[2] Dan Goodin, Why passwords have never been weaker – and crackers have never been stronger, Aug. 20, 2012, http://arstechnica.com/security/2012/08/passwords-under-assault.
[3] See, e.g., Heidi Hoopes, Apps to easily encrypt your text messaging and mobile calls, Gizmag, Sep. 27, 2014, http://www.gizmag.com/secure-text-messaging-phone-clients-comparison-ios-and-android/34000/. See also Services, Silent Circle, https://silentcircle.com/services (last accessed Oct. 31, 2014).
[4] See, e.g., Google Wallet, Google, https://www.google.com/wallet (last accessed Oct. 31, 2014). See also iOS8 Health, Apple, https://www.apple.com/ios/whats-new/health (last accessed Oct. 31, 2014).
[5] Sid Kirchheimer, How to Cyberproof Your Phone, AARP, May 2014, http://www.aarp.org/home-family/personal-technology/info-2014/cyberproof-stolen-phone-kirchheimer.html.
[6] James Comey, Remarks before the Brookings Institution, Federal Bureau of Investigation, Oct. 16, 2014, http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.
[7] Center for Democracy, CALEA II: Risks of Wiretap Modifications to Endpoints, May 17, 2013, pgs. 4-6, https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf.
[8] For example: In 2010, Chinese hackers breached the internal systems that companies like Google and Microsoft use to comply with government search warrants on their users, including the email accounts of suspected terrorists and spies. Ellen Nakashima, Chinese hackers who breached Google gained access to sensitive data, U.S. officials say, Washington Post, May 20, 2013, http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html.

US businesses harmed: Consumers outside of the US may be much less inclined to purchase American tech products that facilitate government surveillance. Consider, for example, the difficulty US companies would have selling smartphones or network servers in the EU that are built to enable easy access for the NSA. As a technical matter, it is difficult and expensive to both build a backdoor security vulnerability and then defend that vulnerability against unauthorized use. This burden would be heaviest on small businesses and innovators of new communications services, which may be create a disincentive to encrypt their products and services, which would reduce the overall security of users.

Government is not "going dark": There is no doubt that some communications are more difficult to intercept than others, and that the FBI has a legitimate concern that criminals and terrorists will gravitate to communications technologies that are more difficult to surveil. However, taken as a whole, the digital revolution has made more data about us available than ever before, and the government has more tools to obtain and analyze that data than ever before. The volume of government surveillance increases almost every year.[9] The claim that companies' increasing adoption of strong encryption by default will suddenly lead to government "going dark" and unable to access critical information is not accurate.[10]

Encryption is not new: Products and software with strong encryption have been freely available to the public – including criminals – for many years, and have not rendered law enforcement helpless to investigate crimes.[11] By recently choosing to encrypt popular smartphones by default, companies are making this security feature easier to use and more accessible to regular smartphone users who do not seek out increased security protection. This change will *reduce* overall crime by protecting all smartphone users, rather than just those who are already security-conscious.

Government has multiple options: If information is encrypted in one place, it is often available from another source. For example, emails or text messages on an encrypted phone can be retrieved from the email service provider or the phone company. Many smartphones are backed up to the cloud, where the data can be obtained from the service provider through legal process. In addition, law enforcement may be able to compel a suspect to decrypt information or devices with a search warrant.[12]

Compelled decryption: The Department of Justice takes the stance that the government can compel the owner of encrypted devices or account, such as a phone or an email account, to decrypt the information it seeks. The government has successfully argued in a number of cases that a warrant permits it to compel decryption.[13] Whether compelled decryption is permissible or is barred by the Fifth Amendment hinges on a range of issues, including whether decryption is "testimonial," whether the existence of the information sought by the government is a "foregone conclusion," and whether immunity for the act of decryption is provided.[14]

Contempt: If an individual refuses an order to decrypt an electronic device, she could be held in contempt of court. When suspects refuse to testify or answer questions, courts can impose coercive and punitive punishments for contempt, including fines and imprisonment. Imprisonment for civil contempt can last for years,[15] or until the order is obeyed. For example, the Third Circuit approved a contempt sentence that lasted 14 years, maintaining that individuals can be confined as long as they refuse a court order they are capable of obeying.[16]

END

For more information, please contact Joseph Lorenzo Hall, Chief Technologist, at joe@cdt.org.

---

[9] US Courts, Authorized Intercepts Granted Pursuant to 18 U.S.C. § 2519 as Reported in Wiretap Reports for Calendar Years 2003 – 2013, http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2013/Table7.pdf (last accessed Nov. 7, 2014).

[10] The Berkman Center for Internet & Society at Harvard University, "Don't Panic. Making Progress on the 'Going Dark' Debate," (January 2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[11] For example, the powerful and popular encryption standard "PGP" was created in 1991. PGP is available free to the public and can be used to encrypt emails, text, images, hard drives, and more. See OpenPGP Alliance, http://www.openpgp.org/index.shtml (last accessed Oct. 31, 2014).

[12] The government must generally obtain a warrant to search a smartphone. See *Riley v. California*, *134* S.Ct. 2473 (2014).

[13] See, e.g., *United States v. Fricosu*, No. 10-CR-00509 (D. Colo. Jan. 23, 2012), http://www.wired.com/images_blogs/threatlevel/2012/01/decrypt.pdf.

[14] Orin Kerr, Encryption and the Fifth Amendment Right Against Self-Incrimination, The Volokh Conspiracy, Jan. 24, 2012, http://volokh.com/2012/01/24/encrytion-and-the-fifth-amendment-right-against-self-incrimination.

[15] See, e.g., *Shillitani v. United States*, 384 U.S. 364 (1966), https://supreme.justia.com/cases/federal/us/384/364/case.html.

[16] *Chadwick v. Janecka*, 302 F.3d 107 (2002), http://law.justia.com/cases/federal/appellate-courts/F3/302/107/560004.

PRIVACY AND SECURITY

Mutual Legal Assistance Treaties (MLAT)

Computer & Communications Industry Association
Tech Advocacy Since 1972

Cross-Border Law Enforcement Demands

The Problem – The Electronic Communications Privacy Act (ECPA) governs the process by which law enforcement (LE) can request disclosure of a subscriber's electronic communications and related information from U.S. service providers. ECPA does not permit direct disclosure of communications by U.S. providers in response to demands from foreign governments, and foreign laws may prohibit U.S. providers that operate abroad from disclosing communications to U.S. law enforcement in response to an ECPA order.

Electronic Communications Privacy Act – Disclosure to U.S. LE under ECPA requires, at minimum and contingent on the type of data requested, a court order. Since the *Warshak* decision in 2010, major service providers have required a warrant for LE access to the contents of communications, and have sought to reform ECPA to permanently enshrine the warrant-for-content standard currently practiced nationwide.

To obtain electronic communications and related digital information pursuant to a criminal investigation stored abroad, U.S. law enforcement must generally make requests to their partners in foreign countries to obtain data through their respective local legal processes, pursuant to the bilateral Mutual Legal Assistance Treaty (MLAT) that governs that information sharing relationship. The MLAT process, characterized as inefficient and time/labor-intensive, is also required in the reverse scenario.

Despites the existing process (or perhaps because of its inefficiencies), providers operating on both sides of the Atlantic have received direct requests from law enforcement for data stored in another jurisdiction, or pertaining to individuals subject to another jurisdiction's laws—leading to conflicts of laws for those providers, and concerns about extraterritorial applicability of U.S. warrants, best exemplified by the "Microsoft-Ireland" case.

Solutions – A variety of bilateral/multilateral international agreements have been suggested to address the conflicts of laws issues resulting from direct LE requests to providers. All would require modifications to ECPA to permit direct disclosure to foreign governments, for which two pieces of legislation have been introduced, with differing approaches.

Solutions based on the *location of the data* sought are problematic because they incentivize data localization and may be technically infeasible for some providers. Forced localization would effectively avoid U.S. authorities and advantage foreign providers. In addition, some providers may not store cloud data in any one location, but may instead utilize "sharding" or "mirroring" systems that keep data in multiple or unknown locations for efficiency reasons.

Law Enforcement Access to Data Stored Abroad (LEADS) Act – The LEADS Act would clarify that U.S. LE cannot compel the disclosure of data from U.S. providers stored abroad if accessing that data would violate the laws of the country where it is stored or if the data is not associated with a U.S. person—that is, a citizen or lawful permanent resident of the United States, or a company incorporated in the United States. Effectively, the *location of the data* sought would govern the legal regime applicable to it.

900 17th Street NW Suite 1100 Washington, DC 20006 P: (202) 783-0070 F: (202) 783-0534 www.ccianet.org

International Communications Privacy Act (ICPA) – ICPA creates a legal framework that authorizes U.S. LE to obtain electronic communications of U.S. persons and persons in the U.S., regardless of where those communications are located. It also allows LE to obtain communications relating to foreign nationals in certain circumstances, where the foreign government does not have a Law Enforcement Cooperation Agreement with the U.S., or if such an agreement exists, the foreign government does not object to disclosure (presumably because the disclosure is either compliant with the terms of such an agreement, or pursuant to a request made by that foreign government). Effectively, the *nationality of the data subject* would govern the legal regime applicable to data sought.

U.S.-U.K. Agreement on Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Countering Serious Crime, Including Terrorism – The U.S.-U.K. Agreement currently being negotiated would permit British authorities to access electronic data directly from U.S. companies where the investigation targets accounts not used by U.S. persons or persons located in the United States. The United States would have reciprocal rights regarding electronic data of U.K. companies or other companies storing data in the United Kingdom, at least to the extent that U.S. laws reach electronic data stored abroad.

Relationship Between ICPA and the U.S.-U.K. Agreement – Legislation would be required to implement the U.S.-U.K. Agreement, given ECPA's general prohibition on disclosure. ICPA is one such bill. It permits the terms of a Law Enforcement Cooperation Agreement to govern disclosure by providers to U.S. law enforcement when U.S. LE is making a request on behalf of a foreign government, pursuant to an agreement like the U.S.-U.K. Agreement.

To qualify, the United Kingdom would have to agree to a number of rules designed to protect privacy and civil liberties, and a U.K. order would have to comply with U.K. law (which operates at a different standard that the U.S. warrant requirement). Significantly, the agreement and implementing legislation would only serve to remove U.S. legal barriers to companies' ability to comply with U.K. orders subject to the agreement. It would not require U.S. companies to comply with a U.K. order; they would remain free to challenge an order or contest U.K. jurisdiction in U.K. courts.

HARMFUL REGULATORY APPROACHES: A CASE STUDY ON PLATFORM REGULATION

REGULATING PLATFORMS? A COMPETITION LAW PERSPECTIVE

by ALFONSO LAMADRID *on* NOVEMBER 24, 2015

Today the two blogs Chillin'Competition and Project DisCo are starting an "inter-platform dialogue" on competition and regulatory matters as regards the digital sector, multi-sided platforms, the digital single market as well as other issues of interest to our readers. Our dialogue will be cross-posted on both blogs. Special thanks to our friend Alfonso Lamadrid from Chillin'Competition who is kicking off the dialogue with his first post below.

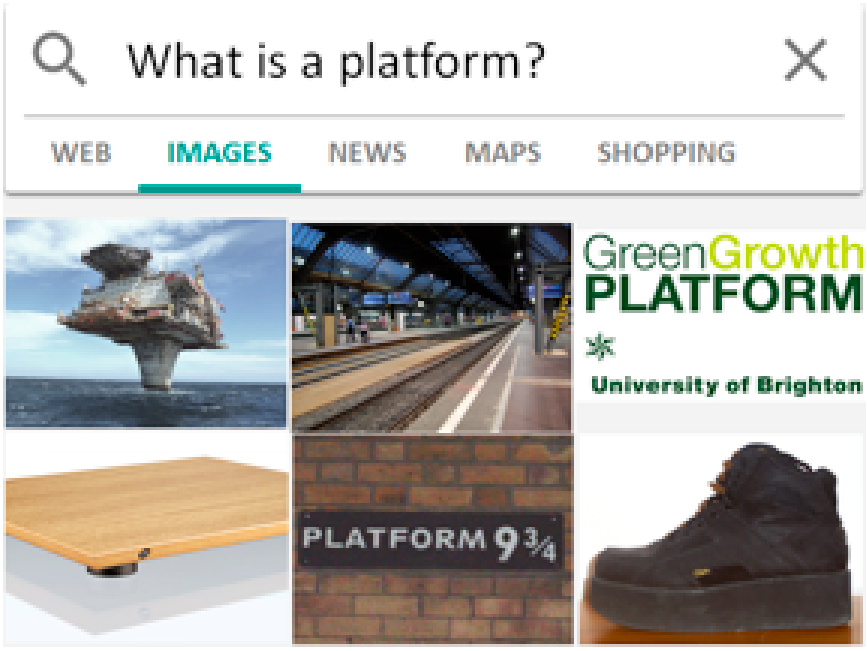
A few days ago I spoke at CEPS about the debate concerning online platform regulation that is attracting some interest these days as DG Connect's and the House of Lords' consultations are ongoing (my presentation and a video interview are available here). This is a most interesting issue although, admittedly, one that not so long ago I would not have expected to be an issue at all.

In the wake of this event we thought that perhaps it would be useful to contribute a bit to the debate, so here you will find a summary of what I said at that conference. In order to complement it, we have decided to engage in a dialogue with our friends at CCIA and their DisCo (Disruptive Competition) Project blog (here or here). This post will also be published here, and we will soon be posting a guest contribution from them. Any comments you might have will certainly enrich the debate.

Not being an expert in regulation, my views on the subject are eminently related to competition law and to its application to multi-sided markets which, as you know, is one of the fields in which I have recently done some work, advising platforms, non-platforms competing with platforms or simply reflecting on wider policy issues (e.g. here or here). The competition law perspective is a particularly useful one because competition law seems to be the elephant in the room, much at the root of these discussions.

Indeed, many of you will recall that *ex ante* "platform" regulation went from being a non-issue to being very much an issue when a number of Member States (notably Germany and France) expressed frustration at how

competition law would not be enough to tackle some problems (not clear which) caused by "some" (apparently not all) platforms (some examples of such statements are available here, here and here). [This concern about the possible shortcomings of competition law coincidentally emerged at a time when some thought that the ongoing Google investigation would fail to establish a "neutrality" obligation incumbent upon Google's search activities] And since competition law was seen as insufficient (read: did not lead to the outcome that some expected), some thought that it would be idea to either change competition law or to bypass it by adopting specific regulation.



What kind of animal is a platform?

In this context, the word "platform" seems to have been chosen to encompass those "some platforms" that people had in mind. However, as explained in previous posts written on the DisCo Project blog (here or here), it may not be the best term to identify a category of companies subject to specific regulation.

Some of you may have heard of the expression "The Law of the Horse". This is a term coined by American judge and antitrust expert Frank Easterbrook in a now famous conference in the US. In this conference he explained that there is no "law of the internet" more than there is a "law of the horse"; that there are laws of contracts that apply when horses are sold, of animal husbandry that apply when they need care, of laws of gambling that regulate when they race, but there is no law of the horse. Nowadays some partisans of regulation are trying to create some sort of "Law of the ~~horse~~ platform". But then of course we come back to the somehow relevant question of what a platform is...

I don't know if you are familiar with the Indian story of "The Blind Men and the Elephant". This is a story in which several blind men are asked to describe what an elephant looks like by touching different parts of its body. The one touching the leg says the elephant is like a pillar; the one touching the belly says it must be like a wall; the one feeling the trunk believes it must look like a tree branch; the one touching the ear is convinced an elephant resembles a hand fan, and so on.. This story illustrates the fallacy that one's subjective experience can be true but at the same time it is inherently limited and cannot account for the totality of the truth.

We see something similar regarding "platforms": some appear to extrapolate certain features or problems from a limited number of companies to a whole business model, but those problems are neither exclusive nor common to "platforms" (as defined in the Commission's consultation). Before doing such a thing, one should perhaps understand how markets work and why companies do what they do.

Having this complete view would certainly be necessary, for, as stated by Easterbrook in his talk *The Law of the Horse*, "*the blind do not make good trailblazers*".

The wrong question

As already noted, the question many are asking is whether competition law is sufficient to address the challenges raised by platforms or whether we need a new framework; does competition law need to adapt?

In my view, and whereas enforcement may need some refinements (e.g. merger notification thresholds may not be well suited for some mergers—see here—and we do not have good economic tools to assess demand-side efficiencies–see here), there is no other branch of law that, over more than a hundred years, has proved similarly flexible, adaptable and accommodating of the evolution of markets and economic thinking than competition law.

In my view, the questions that are being posed now are the wrong ones, so I would suggest that instead of looking at supposed flaws in competition law, perhaps we should look to competition law to extract some lessons.

The above includes understanding why competition authorities are sometimes reluctant to intervene, or why issues that are perceived to be problematic by the lay public are not understood as such by experts in the field. Also, it would be worth reflecting on whether there may be a possibility that if competition law has not done more regarding "platforms" it might be due to the fact that there may indeed be very good reasons for it not to do more.

Why competition law can teach us?

Some may wonder whether competition law can really teach us something about platforms and about how to deal with them. If you ask me, it sure can.

You see, the cornerstone provisions in competition law are merely a couple of articles in the Treaty (or sections in the Sherman Act) and have over the years evolved as interpreted and applied by Courts and specialized agencies to changing markets and in light of mainstream economics free from changing political priorities. Some aura of apparent complexity has also enabled it to evolve soundly, free from the inference of small politics (by which I mean that that its underlying principles are not affected by movable or fashionable political considerations, which is a good thing; by the way, I developed those ideas here). All this has turned competition law into an ever-evolving distillation of common-sense principles infused with mainstream economics.

In addition to that, competition law has a privileged view of the main issues often linked to "platforms". Indeed, many have resorted to our discipline to assess issues such as, for instance, portability and self-favouring (Google case), price restriction in the form of MFNs (several EU and national cases), excessive pricing (see the MIFs cases regarding Visa and Mastercard), interoperability denials (Microsoft) and even privacy considerations in many recent debates and to some extent in *Facebook/Whatsapp*. I can't think of any other discipline having a better view or understanding of what goes on in those settings.

Finally, competition law does not assess all these matters superficially or in the abstract, it analyses them technically and objectively, in specific cases and against the background of factual and economic evidence. Compare that, for instance, with this example of a thoroughly thought out proposal for public intervention... Against this background, ignoring the lessons that competition law experience can offer to the debate would probably not be wise.

What competition law can teach us

- **On whether and how to intervene.** Over the years, experience has taught competition law to be humble, that with great power comes great responsibility, **that authorities should also intervene when a clear problem is identified, and that when they do so they should only act with proportional remedies**. We have come to accept that **markets and competition cannot be perfect, and that is why we aim at "workable" competition; if we strive for perfection, we may be messing with complex realities with unforeseen consequences** (e.g. what is the cost of imposing non-discrimination obligations across the board? Does it make sense? Do we have the knowledge to be sure this is an appropriate remedy?)

- **On the identification of "platforms".** According to the Commission's consultation a platform is essentially an intermediary operating in a two-sided market bringing together different but interdependent groups of users. In competition law there have been plenty of discussions in recent years about how to adapt some of our tools to the peculiarities of two-sided markets. In any given case, and given that many markets present multi-sided features**, the first question that we need to address is whether two-sidedness is enough to matter. And we have come to find that this question is not one that can be answered *ex ante* in the abstract, but on a case-by-case basis and in the light of empirical evidence**. Our experience shows that picking multi-sidedness as the decisive element for specific regulation to apply may be tremendously problematic.

- **On agnosticism towards business models and public distortions**. Over time we have also learnt to move away from the analysis of business models to the assessment of competitive constraints. When we assess a conduct or merger we do not look in isolation at how the business is organized, but at its competitive impact in a relevant market where different business models may compete. **In many markets "online platforms" compete with offline platforms or with non-platforms. Regulating only some of the players active in a market may skew and distort competitive conditions in an undesirable way** (one only needs to look at the "regulatory asymmetry" concerns raised in regard to the sharing economy which is, by the way, subject to the same consultation that also extends to "online platforms"). Competition lawyers are very aware of the fact that most, and the most serious, restrictions of competition often have a public origin.

- ***Ceci n'est pas* market power.** Competition authorities, Courts and lawyers have also learnt to abandon some of our traditional reflexes when it comes to platforms. **We now know that appearances of market power in online settings often cannot be trusted**, because, among others, the markets are extremely dynamic and there are strong actual or potential competitors, services may be provided for free, there may differentiation, multi-homing, easy switching, interoperability or low barriers to entry. **This is not just theory, but also a competitive reality that has been assessed and confirmed in several cases** regarding "online platforms", such as *Google/DoubleClick*, *Microsoft/Skype* (you know my take on that one) or *Facebook/Whatsapp*.

- **Size does not necessarily matter** (this is something that competition lawyers know all too well...) **or that it may not necessarily be a bad thing. Multi-sidedness is about network effects and network effects are a positive externality**; the main defining characteristic of these settings is that scale generates benefits. This also means that:

- **Business practices carried out in multi-sided markets will often be competitively ambiguous,** because the same features that yield market power might help achieve optimal scale/demand side efficiencies (hence the title of my piece on the subject: the double duality of two-sided markets). **Certainly some practices will be anticompetitive also in these settings, but this is something that will have to be looked at carefully and on a case-by-case basis, but is not something that can be decided in the abstract.** This was actually the main message of the ECJ in *Cartes Bancaires*, and once again seems to reveal that *ex ante* regulation may not be ideal.

- **Competition law is always there**, ready to kick in in those specific cases where there things go wrong and there may be problems felt in markets. As noted earlier, we have seen this with portability restrictions, interoperability denials, pricing restrictions, excessive pricing, etc.

- **But competition law isn't the answer to every problem.** Despite the above, over the years we have also come to realize that **competition law is not the answer to every problem.** Expecting the contrary indeed might lead to frustration or to a feeling of insufficiency. This is a message in which I have insisted repeatedly in the context of the debate on the role of competition policy in addressing data protection/privacy concerns (see here among others).

- **On consumer choice as the bottom line.** Competition law is about consumer choice, much like, at least in my view, public policy should be about enabling informed choices. If you ask me, the best way of protecting consumers from the perceived problems in these markets would mainly require informing/educating them, and then making sure that they are not artificially locked-in to a given platform (which is what competition law is here to do in these and other markets). It is often said that "platforms" are powerful because of the information they control; but if information is power, we should perhaps also give it to consumers...

Alfonso Lamadrid is a competition lawyer at Garrigues in Brussels and author of the blog Chillin'Competition. He has extensive expertise in the technology sector and has authored influential works on multi-sided markets.

FURTHER READING

Andrew K. Woods, ***Data Beyond Borders: Mutual Legal Assistance in the Internet Age***, Global Network Initiative
https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf

Anupam Chander, ***How Law Made Silicon Valley***, Emory Law Journal
http://law.emory.edu/elj/content/volume63/issue3/articleshowlawmadesiliconvalley.html

Bruce Schneier, ***The Value of Encryption***
https://www.schneier.com/essays/archives/2016/04/the_value_of_encrypt.html

CCIA, ***Primer: Issues in International Digital Trade***
http://www.ccianet.org/wpcontent/uploads/2017/05/CCIAPrimeronDigitalTradeIssues.pdf

Competition Policy International, ***Internet Competition and Regulation of Online Platforms***
https://www.competitionpolicyinternational.com/wpcontent/uploads/2016/05/INTERNETCOMPETITIONLIBRO.pdf

Daniel O'Connor & Matthew Schruers, ***Against Platform Regulation***
http://ipp.oii.ox.ac.uk/sites/ipp/files/documents/OConnorSchruers%2520%2520Against%2520Platform%2520Regulation.pdf

Georgia Tech, ***Cross-Border Requests for Data Project***
http://www.iisp.gatech.edu/crossborderdataproject

Global Network Initiative, ***GNI Principles on Freedom of Expression and Privacy***
https://globalnetworkinitiative.org/sites/default/files/GNIPrinciplesonFreedomofExpressionandPrivacy_0.pdf

Google, ***How Google Fights Piracy***
https://drive.google.com/file/d/0BwxyRPFduTN2TmpGajJ6TnRLaDA/view

Harold Abelson et al., ***Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communication***
https://dspace.mit.edu/bitstream/handle/1721.1/97690/MITCSAILTR2015026.pdf

Ian Brown et al ., ***Reforming Mutual Legal Assistance Needs Engagement Beyond the U.S.***, Lawfare
https://www.lawfareblog.com/reformingmutuallegalassistanceneedsengagementbeyondus

Internet Association, ***The Regulatory Environment for Platforms, Online Intermediaries, Data and Cloud Computing and the Collaborative Economy***
https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/573d2a2b7c65e401e661831f/1463626284158/IAMemo.pdf

Ira Magaziner, ***A Framework for Global Electronic Commerce***
https://clinton4.nara.gov/WH/New/Commerce/read.html

ITI, ***Global Guiding Principles for Trust, Technology and Government Access in the Digital Age***
http://www.itic.org/dotAsset/8/0/80ec80e7789842b095db6c4d4a57e932.pdf

James Manyika et al ., ***The Internet of Things: "Mapping the Value Beyond the Hype***, McKinsey
http://www.mckinsey.com/businessfunctions/digitalmckinsey/ourinsights/theinternetofthingsthevalueofdigitizingthephysicalworld

Jennifer Daskal & Andrew Keane Woods, ***CrossBorder Data Requests: A Proposed Framework***, Lawfare
https://lawfareblog.com/crossborderdatarequestsproposedframework

Kevin Bankston, ***The Numbers Don't Lie***, Slate
http://www.slate.com/articles/technology/future_tense/2015/08/default_smartphone_encryption_will_stop_more_crimes_than_it_permits.html
Laura Adler, ***How Smart City Barcelona Brought the Internet of Things to Life***, DataSmart City Solutions
http://datasmart.ash.harvard.edu/news/article/howsmartcitybarcelonabroughtheinternetofthingstolife789
Marvin Ammori, ***The Music Industry Sings a Lonely Tune on Internet Policy***, The Hill
http://thehill.com/blogs/congressblog/judicial/284987themusicindustrysingsalonelytuneoninternetpolicy
Peter Swire & Deven Desai, ***A "Qualified SPOC" Approach for India and Mutual Legal Assistance***, Lawfare
https://www.lawfareblog.com/qualifiedspocapproachindiaandmutuallegalassistance

TECH TRADE ASSOCIATIONS AND OTHER STAKEHOLDERS

Application Developers Alliance: www.appdevelopersalliance.org

Center for Democracy and Technology (CDT): www.cdt.org

CompTIA: www.comptia.org

Computer and Communications Industry Association (CCIA): www.ccianet.org

Consumer Technology Association (CTA): www.cta.tech

Engine: www.engine.is

Global Innovation Forum: globalinnovationforum.com

Global Network Initiative (GNI): www.globalnetworkinitiative.org

Information Technology Industry Council (ITI): www.itic.org

Information Technology Industry Foundation (ITIF): itif.org

Interactive Advertising Bureau (IAB): www.iab.com

Internet Association (IA): internetassociation.org

Internet Infrastructure Coalition (i2C): www.i2coalition.com

NetChoice: netchoice.org

Public Knowledge: www.publicknowledge.org

R Street Institute: www.rstreet.org

Re:Create Coalition: www.recreatecoalition.org

Software Information Industry Association (SIIA): www.siia.net

TechNet: technet.org

Tech:NYC: www.technyc.org

US Chamber of Commerce: www.uschamber.com

Fundamentals of Internet Policy