



## Public Interest Comment

---

*Comments submitted to the National Telecommunications and Information Administration in the Matter of:*

# Digital Economy Board of Advisors Meeting

Ryan Hagemann

Technology and Civil Liberties Policy Analyst  
The Niskanen Center

Submitted: December 9, 2016  
Docket No. NHTSA-2016-28708

---

## Executive Summary

These comments will address the issues of promoting trust online and innovation and emerging technologies. To that end, we offer a research paper from the Niskanen Center (“Encryption, Trust, and the Online Economy: An Assessment of the Economic Benefits Associated with Encryption”), submitted as a separate attachment, that focuses on the issue of online trust in great detail. Additionally, we cite numerous comment filings on a wide array of topics—from autonomous vehicles to content delivery networks—in addressing the question of how regulators can most effectively promote emerging technologies without negatively impacting innovation.

---

*The Niskanen Center is a 501(c)3 libertarian issue advocacy organization that works to change public policy through direct engagement in the policymaking process.*

THE NISKANEN CENTER | 820 FIRST ST. NE, SUITE 675 | WASHINGTON, D.C. 20002  
[www.niskanencenter.org](http://www.niskanencenter.org) | For media inquiries, please contact [ltavlas@niskanencenter.org](mailto:ltavlas@niskanencenter.org)

## Introduction

As Larry Downes pointed out in a recent *Washington Post* op-ed, “slow-moving regulators, even with the best of intentions, can do very little good trying to shape a digital revolution already in progress.”<sup>1</sup> As the Digital Economy Board of Advisors meet to recommend policies on preserving and extending the growth of the digital economy to the Secretary of Commerce, Mr. Downes’ words should be at the forefront of participants’ minds.

While the Niskanen Center supports efforts at promoting a free and open Internet across the globe and ensuring digital access for workers, families, and companies, we will confine our comments to the two areas in which we have more extensive research and advocacy experience: promoting trust online and promoting innovation and emerging technologies.

## Promoting Trust Online

One of the lowest-cost mechanisms that yields high returns on ensuring trust in the online ecosystem is the use of encryption, both end-to-end (E2E) and transit layer security (TLS). As we discuss in a 2015 paper, encryption has served a valuable role in promoting online trust and its proliferation has contributed mightily to the growth of the digital economy: “In 1994, total online business transactions were estimated at around \$100 million. By 2000 the U.S. Department of Commerce predicted a 3,000-fold increase in the ecommerce sector to \$300 billion.” As of 2014, total e-commerce retail sales had indeed amounted to well over \$300 billion, annually.<sup>2</sup>

To put these numbers in perspective, total U.S. Gross Domestic Product was approximately \$14.5 trillion in 2012, of which the Internet’s contribution is estimated to have been \$681 billion—almost 5 percent of GDP.<sup>3</sup> In our paper, we outline how trust has been improving in the online digital landscape, from banking to e-commerce. It is notable that the rise of mobile platforms for finance and e-commerce have seen the greatest increase in user trust, especially among younger cohorts. As smartphones become cheaper, more powerful, and home to a wider array of services and apps, this ecosystem will likely continue to see soaring user adoption rates; that is, assuming government actors abstain from imposing costly and ineffective barriers to the adoption of encryption.

---

<sup>1</sup> Larry Downes, “How Should Donald Trump’s Administration Regulate the Internet?,” *The Washington Post*, November 30, 2016, [https://www.washingtonpost.com/news/innovations/wp/2016/11/30/how-should-donald-trumps-administration-regulate-the-internet/?utm\\_term=.366b01f01450](https://www.washingtonpost.com/news/innovations/wp/2016/11/30/how-should-donald-trumps-administration-regulate-the-internet/?utm_term=.366b01f01450).

<sup>2</sup> Ryan Hagemann and Josh Hampson, “Encryption, Trust, and the Online Economy: An Assessment of the Economic Benefits Associated with Encryption,” Niskanen Center, November 9, 2015, [https://niskanencenter.org/wp-content/uploads/2015/11/RESEARCH-PAPER\\_EncryptionEconomicBenefits.pdf](https://niskanencenter.org/wp-content/uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf).

<sup>3</sup> David Dean, Sebastian DiGrande et. al., “The Internet Economy in the G-20,” BCG Perspectives, March 19, 2012, [https://www.bcgperspectives.com/content/articles/media\\_entertainment\\_strategic\\_planning\\_4\\_2\\_trillion\\_opportunity\\_internet\\_economy\\_g20/](https://www.bcgperspectives.com/content/articles/media_entertainment_strategic_planning_4_2_trillion_opportunity_internet_economy_g20/). (The total contribution of the Internet to GDP was calculated as 4.7 percent of the given \$14.5 trillion GDP numbers [(0.047)(\$14,500,000,000) = \$681,500,000,000]).

Over the past two years, battles over whether to expand law enforcement access to E2E devices have been playing out in news headlines.<sup>4</sup> Although law enforcement agencies have reasonable concerns surrounding the potential for various communications platforms “going dark,” regulations or legislation<sup>5</sup> that would force companies to hold encryption keys—or worse, the plain text conversations and communiques between individuals—would have an injurious effect on people’s willingness to trust online service providers. In addition, the reality is that many encryption providers are foreign-based or open-source, severely limiting the ability of policymakers to simply “legislate away” the encryption debate.<sup>6</sup>

For all these reasons, the Niskanen Center has long supported the Digital Security Commission, proposed by House Homeland Security Chairman Michael McCaul and Sen. Mark Warner.<sup>7</sup> This bipartisan legislation would establish a Congressionally-backed commission that would include all relevant stakeholders—from economists and cryptographers to law enforcement agencies and the intelligence community—and charge them with hammering out the details of what can be done to ensure the preservation of online security, while addressing the many real and considerable concerns faced by the law enforcement community.

Encryption is unique in its ability to engender trust amongst online users. Its continued use and prevalence will be a necessary precondition for the continued growth of trust online. Weakening encryption, through legislation or regulatory fiat, will only result in loss of consumer faith in the online ecosystem, and would likely have disastrous consequences for the modern digital economy.

## Promoting Innovation and Emerging Technologies

Given Alan Davidson’s presentation at the May 2016 DEBA meeting,<sup>8</sup> we will confine our comments on emerging technologies to those areas the board intends to focus their initial attention on: the Internet of Things (IoT), autonomous vehicles, and commercial unmanned aerial systems (UAS).

---

<sup>4</sup> See generally Ryan Hagemann, “Missing the Forest for the Apple Tree,” Niskanen Center, February 22, 2016, <https://niskanencenter.org/blog/missing-the-forest-for-the-apple-tree/>.

<sup>5</sup> In particular, we are referencing the Compliance with Court Orders Act, co-sponsored by Sens. Dianne Feinstein and Richard Burr, which holds in part that “a covered entity that receives a court order ... shall be responsible only for providing data in an intelligible format if such data has been made unintelligible by a feature, product, or service owned, controlled, created, or provided, by the covered entity or by a third party on behalf of the covered entity.” Unfortunately, such a mandate holds the potential to do significant damage to the security and trust of online users. For more on our specific criticisms, see: Ryan Hagemann, “Burr and Feinstein: To Hell With Encryption,” Niskanen Center, April 8, 2016, <https://niskanencenter.org/blog/burr-and-feinstein-to-hell-with-encryption/>.

<sup>6</sup> Bruce Schneier, “Worldwide Encryption Products Survey,” Schneier on Security Blog, February 11, 2016, [https://www.schneier.com/blog/archives/2016/02/worldwide\\_encry.html](https://www.schneier.com/blog/archives/2016/02/worldwide_encry.html). (“The findings of this survey identified 619 entities that sell encryption products. Of those 412, or two-thirds, are outside the U.S.—calling into question the efficacy of any US mandates forcing backdoors for law-enforcement access.”)

<sup>7</sup> See generally “McCaul-Warner Commission on Digital Security,” House Homeland Security Committee, <https://homeland.house.gov/mccaul-warner-commission-2/>.

<sup>8</sup> Alan Davidson, “Commerce Department Digital Economy Agenda 2016,” May 2016, Presentation, [https://www.ntia.doc.gov/files/ntia/publications/alan\\_davidson\\_digital\\_economy\\_agenda\\_deba\\_presensation\\_0516\\_16.pdf](https://www.ntia.doc.gov/files/ntia/publications/alan_davidson_digital_economy_agenda_deba_presensation_0516_16.pdf).

## *The Internet of Things*

One of the great challenges currently facing regulators centers on the rapid emergence and profusion of new technologies. How can regulators hope to fulfill their statutory mandates to protect the public interest when confronted with technologies that outpace the traditional slow-crawl of the regulatory process, all while preserving the innovation and economic growth engendered by the modern digital economy? The answer is that agencies need to embrace new frameworks, processes, and rules for addressing the potential concerns posed by emerging technologies. To that end, the Niskanen Center recently proposed a framework that can provide a starting point in a larger conversation surrounding regulatory reform.

In comments submitted to the National Telecommunications and Information Administration (NTIA) on the role of the government in the IoT, we argued: “The tenets of the ‘Framework for Global Electronic Commerce’ should guide the federal government’s approach to regulating the IoT.”<sup>9</sup> This framework, originally promulgated by the Clinton Administration, was geared towards ensuring the continued growth of the commercial Internet. For the past two decades it has served the Internet marketplace, and stood the test of time, marvelously well. Although we retailored the language to apply specifically to the IoT, the following tenets can serve as a solid foundation for best practices when approaching any new emerging technology:

1. **“The private sector should lead.”** The framework specifies that “governments should encourage industry self-regulation wherever appropriate and support the efforts of private sector organizations to develop mechanisms to facilitate the successful operation of the” IoT. “Even where collective agreements or standards are necessary, private entities should, where possible, take the lead in organizing them.”
2. **“Governments should avoid undue restrictions” on the IoT.** “Unnecessary regulation of commercial activities will distort development of the electronic marketplace by decreasing the supply and raising the cost of products and services for consumers. ... [G]overnment attempts to regulate are likely to be outmoded by the time they are finally enacted, especially to the extent such regulations are technology-specific. Accordingly, governments should refrain from imposing new and unnecessary regulations, bureaucratic procedures, or taxes and tariffs on commercial activities that take place via the” IoT.
3. **“Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce.”** The framework specifies that “where government intervention is necessary to facilitate” the development of the IoT, “its goal should be to ensure competition, protect intellectual

---

<sup>9</sup> Ryan Hagemann, *Comments submitted to the National Telecommunications Information Administration in the Matter of: The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, NTIA Docket No. 160331306-6306-01, submitted May 23, 2016, [https://niskanencenter.org/wp-content/uploads/2016/05/NiskanenCenter\\_NTIA\\_IoT\\_Comments.pdf](https://niskanencenter.org/wp-content/uploads/2016/05/NiskanenCenter_NTIA_IoT_Comments.pdf).

property and privacy, prevent fraud, foster transparency, support commercial transactions, and facilitate dispute resolution.”

4. **“Governments should recognize the unique qualities of the” IoT.** “Regulation should be imposed only as a necessary means to achieve an important goal on which there is broad consensus. Existing laws and regulations that may hinder electronic commerce [and the continued development of the IoT] should be reviewed and revised or eliminated to reflect the needs of the new electronic age.”<sup>10</sup>

Cybersecurity is a primary concern when discussing not just the IoT, but many new technologies, from autonomous vehicles to commercial drones. However, as discussed in a recent Niskanen Center blog on this topic:

*We need to focus on cybersecurity as a “service,” not a mandatory obligation. There are no silver bullets to the problem of cybersecurity, but there are learning experiences, and we should treat each breach, attack, and intrusion as an opportunity to learn from mistakes, not create new ones with knee-jerk regulations.*<sup>11</sup>

Insurance and industry self-regulating mechanisms can be far more effective solutions to these problems. This is especially so when considering the need for retaining flexibility in an ever-changing landscape like the IoT. A better solution, if regulators seek to act in an *ex ante* fashion, would be to assess where liability could be most appropriately situated in order to help guide individuals and firms to make better decisions regarding the security of their products and services. Top-down regulatory fiat, however, should be avoided as a measure of absolute last resort and held to a high standard of cost-benefit analysis.

## *Autonomous Vehicles*

Autonomous vehicles hold the potential to massively disrupt the transportation industry, bringing with it numerous benefits to public health, the environment, and congestion.<sup>12</sup> Given those potential upsides, regulators should abstain from constructing onerous and prescriptive rules for manufacturers, software engineers, designers, and testers of these vehicles, as well as the associated technologies. The best rules for a complex world are generally the simplest, and the National Highway Traffic Safety Administration (NHTSA), which is charged with overseeing the safety of American roadways, should bear this in mind when confronting the issue of autonomous vehicles.

---

<sup>10</sup> Ryan Hagemann, *Fostering the Advancement of the Internet of Things*.

<sup>11</sup> Ryan Hagemann, “2017 Policy Priorities: Making Way for the Internet of Everything,” Niskanen Center blog, November 30, 2016, <https://niskanencenter.org/blog/2017-policy-priorities-making-way-internet-everything/>.

<sup>12</sup> See generally Adam Thierer and Ryan Hagemann, “Removing Roadblocks to Intelligent Vehicles and Driverless Cars,” Mercatus Working Paper, Mercatus Center, September 2014, <https://www.mercatus.org/system/files/Thierer-Intelligent-Vehicles.pdf>.

NHTSA is already in the early stages of addressing the many issues associated with autonomous vehicles, and recently solicited feedback on its proposed guidelines for a federal automated vehicle policy. In its own comments, the Niskanen Center argued against proposed pre-market approval authorities and post-sale authority to regulate software changes, while supporting the continuation of the self-certification process that has served the agency well over its many decades overseeing the safety of American roadways.<sup>13</sup> Other commenters have expressed similar concerns and recommended the agency abstain from extending its statutory authority into new territory.<sup>14</sup>

In a report intended to guide the thinking of policymakers and regulators on these matters, the RAND corporation noted that regulators face a daunting challenge:

*First, regulatory promulgation is fundamentally an iterative and slow process, given the cycles of proposals, requests for comments, reviews, and lobbying that precede rulemaking. Second, with [autonomous vehicle] technologies in particular, their newness and rapid evolution create uncertainty in both rulemaking effects and of the technology itself. Moreover, with rapid technology changes, it can be challenging to prescribe rules that will remain relevant and appropriate through the development process. A government transportation official we interviewed stated that, when it came to issuing standards, he thought it was extremely difficult to stay relevant, given the swift pace of technological change.*<sup>15</sup>

The RAND report's conclusion best sums up our feelings on the matter of autonomous vehicles:

*[T]he guiding principle for policymakers should be that AV technology should be permitted and encouraged if and when it is superior to average human drivers. So, for example, safety regulations and liability rules should be designed with this overarching guiding principle in mind. ... This stands in contrast to an alternative approach of viewing AVs with more suspicion and requiring near perfection before introduction.*<sup>16</sup>

We understand the need to weigh the public interest with the many benefits this technology. However, an expansion of NHTSA's authority, especially to permit pre-market approvals, is not the

---

<sup>13</sup> Ryan Hagemann, *Comments submitted to the National Highway Traffic Safety Administration in the Matter of: Federal Automated Vehicle Policy*, Niskanen Center, NHTSA Docket No. 2016-0090, submitted November 22, 2016, <https://niskanencenter.org/wp-content/uploads/2016/11/CommentsAutonomousVehicleStandardsNHTSA.pdf>.

<sup>14</sup> Ian Adams, Berin Szoka, and Marc Scribner, *Comments of the Competitive Enterprise Institute, R Street Institute, and TechFreedom in the Matter of Request for Comments on Federal Automated Vehicles Policy*, NHTSA Docket No. 2016-0090, submitted November 22, 2016, <http://www.rstreet.org/wp-content/uploads/2016/11/CEI-et-al-NHTSA-FAVP-guidance-comments.pdf>; Adam Thierer and Caleb Watney, *Comment on the Federal Automated Vehicles Policy*, Mercatus Center, submitted November 22, 2016, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2876832](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2876832).

<sup>15</sup> James M. Anderson, Nidhi Kalra, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras, Oluwatobi A. Oluwatola, "Autonomous Vehicle Technology: A Guide for Policymakers," RAND Corporation, 2014, p. 139.

<sup>16</sup> RAND, "Autonomous Vehicle Technology," p. 145.

correct avenue for striking this balance. The most appropriate course of action lies not in regulating the technology in question, but rather focusing on addressing where liability lies in the event of an accident.<sup>17</sup> That will do far more to provide market certainty, while ameliorating the public interest consideration of NHTSA’s mandate, than any of the agency’s recently proposed authorities.

## *Commercial Unmanned Aerial Systems*

The same issues facing autonomous vehicles on the roadways are also at play in the push to integrate commercial drones in the national airspace. After a long three years, and numerous missed deadlines, the Federal Aviation Administration (FAA) finally released its long-awaited rules governing the operations of commercial UAS last year. While they go a long way towards creating an environment of reasonable regulatory certainty for market actors, many of the rules are innovation-killers. In particular, the major provisions that are cause for concern include:

- Restrictions on flying UAS beyond the visual line-of-sight of operators;
- Limiting operators to flying one drone at a time;
- Permitting operations during daylight-only hours; and
- Restrictions on flights over individuals not involved in the operation of the drone.

These restrictions and limitations do not take account of the current state of technological development, much less the likelihood of advanced automation systems that could effectively address potential harm scenarios.<sup>18</sup> Had the FAA conducted a thorough cost-benefit analysis accounting for these realities, it likely would have arrived at a less prescriptive regulatory regime—and one which would be less likely to frustrate efforts to begin working towards drone delivery services, vertical take-off and landing transportation, and other, yet undreamt of possibilities.<sup>19</sup> It will also be necessary to consider how air traffic control reform can fit into the larger picture of UAS operations—an issue that has received lackluster attention.

---

<sup>17</sup> John Villasenor, “Products Liability and Driverless Cars: Issues and Guiding Principles for Legislation,” Brookings Institution, April 2014, p. 16, [https://www.brookings.edu/wp-content/uploads/2016/06/Products\\_Liability\\_and\\_Driverless\\_Cars.pdf](https://www.brookings.edu/wp-content/uploads/2016/06/Products_Liability_and_Driverless_Cars.pdf). (“Liability for vehicle manufacturing defects has always been the province of state courts applying state tort remedies. That should continue to be the case for autonomous vehicles. While it is certainly true that state court remedies are sometimes inconsistent, it does not follow that the solution is for the federal government to strip state courts of their authority. Among other problems, federal preemption would put the federal government in the impossible position of trying to formulate the ‘right’ set of liability standards that would then be imposed, including the inevitable mistakes they would contain, on the states.”)

<sup>18</sup> Eli Dourado, Ryan Hagemann, and Adam Thierer, *Comments of the Mercatus Center at George Mason University in the matter of the Operation and Certification of Small Unmanned Aircraft Systems*, Mercatus Center, Docket No. FAA-2015-0150, submitted April 24, 2015, <http://mercatus.org/sites/default/files/Dourado-UAS-PIC.pdf>;

<sup>19</sup> Adam Thierer and Ryan Hagemann, *Comments of the Mercatus Center at George Mason University in the matter of the FAA Interpretation of the Special Rule for Model Aircraft*, Mercatus Center, Docket No. FAA-2014-0396, submitted September 23, 2014, <http://mercatus.org/publication/federal-aviation-administration-interpretation-special-rule-model-aircraft-0>.

There are also non-FAA issues at play, such as privacy considerations. However, as the Niskanen Center noted in brief comments filed to the Federal Trade Commission (FTC), UASs do not present unique privacy concerns that require heavy-handed action.<sup>20</sup> In fact, the emergence of consensus-based standards have served the development of this space quite well. The FTC is already well equipped to address consumer harms after the fact, and a network of state law, criminal codes, and local ordinances can effectively remedy privacy concerns.

## Conclusion

Regulators are currently ill-equipped to appropriately respond to the challenge faced by autonomous vehicles, as well as emerging technologies more broadly, given their current toolkits. Many of these agencies were erected in a day and age when the rate of technological change was far less pronounced. Regulatory agencies are simply not capable of promulgating effective, balanced *ex ante* rules governing the rapid, transformative innovation economy. As a result, reform is desperately needed, lest archaic rules and regulatory accumulation deny the wider public of the many benefits of these emerging marvels.<sup>21</sup>

As a final note, we applaud the Board’s focus on “ensuring the Internet continues to thrive as an engine of growth, innovation, and free expression” and look forward to its recommendations.<sup>22</sup>

We thank the Digital Economy Board of Advisors for the opportunity to submit these comments and look forward to future opportunities for collaboration.

---

<sup>20</sup> Ryan Hagemann, *Comments submitted to the Federal Trade Commission in the Matter of: The Privacy Implications of Commercial Drone Operations*, Niskanen Center, FTC Seminar Addressing Drones, submitted November 13, 2016, <https://niskanencenter.org/wp-content/uploads/2016/11/CommentsDronePrivacyRulesFTC.pdf>; Berin Szoka, Tom Struble, and Ben Sperry, *Comments of TechFreedom in the matter of Privacy, Transparency, and Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems*, TechFreedom, NTIA Docket No. 150224183-5183-01, April 20, 2015, [http://www.ntia.doc.gov/files/ntia/techfreedom\\_4.20.15.pdf](http://www.ntia.doc.gov/files/ntia/techfreedom_4.20.15.pdf).

<sup>21</sup> For a broader account of what ideal first-steps towards reform would entail, we suggest the following policy memo: Michael Mandel and Diana G. Carew, “Regulatory Improvement Commission: A Politically-Viable Approach to U.S. Regulatory Reform,” Progressive Policy Institute, May 2013, [http://www.progressivepolicy.org/wp-content/uploads/2013/05/05.2013-Mandel-Carew\\_Regulatory-Improvement-Commission\\_A-Politically-Viable-Approach-to-US-Regulatory-Reform.pdf](http://www.progressivepolicy.org/wp-content/uploads/2013/05/05.2013-Mandel-Carew_Regulatory-Improvement-Commission_A-Politically-Viable-Approach-to-US-Regulatory-Reform.pdf).

<sup>22</sup> Notice of the Federal Register, Vol. 81, No. 229 p. 85937, posted November 29, 2016, <https://www.gpo.gov/fdsys/pkg/FR-2016-11-29/pdf/2016-28708.pdf>.

# Encryption, Trust, and the Online Economy

An Assessment of the Economic Benefits Associated With Encryption

---

BY RYAN HAGEMANN AND JOSH HAMPSON

## EXECUTIVE SUMMARY

The problems of online security and the non-economic benefits of encryption are well understood, but there has yet to be a comprehensive analysis of the economic benefits created by the spread of encryption. This is not surprising. When encryption is working properly, the user is not even aware of its existence.

In order to gauge the overall benefits of encryption, we examined five separate metrics that rely on encryption: (1) online banking and financial transactions, (2) e-Commerce and online retail, (3) information communication technologies (ICT) security revenue, employment, and insurance, (4) research and development investment, and (5) consumer surplus. In each of these areas, the available data indicates strong growth trends over the past quarter century. In some situations the growth has been profound. The growth of e-Commerce, for example, has skyrocketed from total annual sales of \$100 million in 1994 to over \$250 billion as of 2009.

Although e-Commerce has seen some of the most significant growth, the final concluding graph will show that each of these metrics has grown precipitously over the observed years. The one exception to this trend is consumer surplus. As we discuss, consumer surplus is a difficult measure to standardize for analysis and among all the metrics examined, is the least informative of the value of encryption in the online ecosystem.

It's not possible to say precisely how much of this growth is due specifically to the wide availability and use of secure encryption. However, it is exceedingly unlikely that these sectors would have boomed as they did without the assurance of security that encryption provides. Even if the specific contribution of encryption in the growth of these fields is proportionately small, the scale of these increases is so large that even a small contribution would be large, and economically significant, in absolute terms. Future work is needed to more precisely specify how much of this observed growth is owed specifically to encryption.

## INTRODUCTION

In 1984, 8.2 percent of all American homes had a computer. By 2012, that number had jumped to almost 80 percent, with 95 percent of those homes using it to connect to the Internet. In 1997, only 18 percent of those with computers had Internet access. As of 2012, 75 percent of all households had Internet access at home.<sup>1</sup> The Internet and communications technologies have grown explosively over the past three decades. The growth of mobile networks and the increasing affordability of smartphones has contributed significantly to the spreading global reach of the Internet. As Internet use continues to grow, the importance of encryption in safeguarding the data that consumers transmit online, whether for storage in the cloud or for commercial and financial transactions, will grow along with it.

Without encryption, secure transfer protocols (SSL and TLS) would not exist, which would leave hundreds of millions of online consumers' financial, health, and personal information open to eavesdropping and theft. Interbank payment processing would be vulnerable to "man-in-the-middle" attacks, whereby malicious agents siphon off unencrypted communications in transit. In short, the modern economy would be significantly weakened by the deployment of less-than-optimally secure encryption—to the detriment of individuals, businesses, and government agencies.

A comprehensive accounting of all the economic impact of encryption technology would require a book rather than a short paper. This study is of limited scope and ambition, aiming only to arrive at only an educated guess about the economic benefits of encryption. We try to define a framework and specify some metrics that will be useful for arriving at a reasonable rough estimate. We hope this will serve as useful first step toward a deeper understanding of the role and value of encryption in the modern digital economy.

## FOUNDATIONAL ANALYSIS

In the midst of the exploding commercial growth of the Internet, the National Institute for Standards and Technology (NIST) produced a study assessing the net present value (NPV) of encryption. It concluded that, as of 2001, the NPV ranged from \$345 billion to \$1.2 trillion, in 2001 dollars. It also provided a cost-benefit analysis of the use of the Data Encryption Standard (DES) from 1973 to 1982, which, as the accompanying graph shows, resulted in decreasing costs and increasing benefits over the decade long period.

---

<sup>1</sup> United States Census Bureau, "Measuring America," Feb. 3, 2014.  
[https://www.census.gov/hhes/computer/files/2012/Computer\\_Use\\_Infographic\\_FINAL.pdf](https://www.census.gov/hhes/computer/files/2012/Computer_Use_Infographic_FINAL.pdf)

**Table 20. Constant Dollar (Yr. 2000) Benefits and Costs, 1973-1982\***

| <b>Year</b> | <b>Benefits<br/>(Constant 2000 Dollars)</b> | <b>Costs<br/>(Constant 2000 Dollars)</b> | <b>Net Benefits<br/>(Constant 2000 Dollars)</b> |
|-------------|---|--|---|
| 1973        | 0   | 300,000                                  | (300,000)                                       |
| 1974        | 0   | 800,000                                  | (800,000)                                       |
| 1975        | 0   | 900,000                                  | (900,000)                                       |
| 1976        | 0   | 900,000                                  | (900,000)                                       |
| 1977        | 73,166,519                                  | 700,000                                  | 72,466,519                                      |
| 1978        | 99,581,224                                  | 425,000                                  | 99,156,224                                      |
| 1979        | 137,871,618                                 | 500,000                                  | 137,371,618                                     |
| 1980        | 178,360,272                                 | 320,000                                  | 178,040,272                                     |
| 1981        | 212,868,471                                 | 220,000                                  | 212,648,471                                     |
| 1982        | 281,902,880                                 | 220,000                                  | 281,682,880                                     |

\* The deflator used to convert current to constant dollars is the Gross Domestic Product Price Index (chain type), Economic Report of the President, 20001, Table B7.

The government's assessment of the value of this early digital encryption standard suggests that its impact would be even greater today. The massive and unprecedented growth of ICT over the past quarter-century hints at the extent of the need for secure means of using those networks. Unfortunately, the government has not undertaken an assessment of both the economic costs and benefits of encryption since this 2001 report, in which the time-series data end in the early 1980s, just as the Internet's early progenitor was taking off. There is no government estimate of the value of encryption since the Internet's commercialization in the early 1990s. However, there is reason to believe that economic value of encryption is very large.

At the firm level, the use of encryption can be immensely beneficial. Forrester Consulting estimated the overall costs and benefits of a firm implementing Pretty Good Privacy (PGP) protections to be substantial. Using their Total Economic Impact (TEI) model and customer interviews, Forrester estimated that the risk-adjusted return on investment (ROI) for using the PGP encryption platform was 162 percent. The NPV was estimated to be \$1,363,325.<sup>2</sup> When compared to alternative approaches to data security, Forrester concluded that with the use of PGP firms "can see significant cost savings and capital expenditure reductions."<sup>3</sup>

From a more macroeconomic perspective, the economic contribution of the ICT market has been profound. As of 2012, the Internet accounted for 4.7 percent of U.S. Gross Domestic Product (GDP), according to a report from the Boston Consulting Group. Total

<sup>2</sup> The total costs amounted to \$843,137 and total benefits were \$2,206,462. Jeffrey North and Michelle Salazar, *The Total Economic Impact Of PGP Encryption Platform Within A Global Media Company*, Forrester Consulting, prepared for PGP Corporation, March 2008.

<sup>3</sup> Jeffrey North and Michelle Salazar, *The Total Economic Impact Of PGP Encryption Platform Within A Global Media Company*, Forrester Consulting, prepared for PGP Corporation, March 2008.

GDP in 2012 was \$14.5 trillion, putting the Internet's contribution to national economic output at around \$681 billion.<sup>4</sup>

Over the past quarter century, the Internet's contribution to U.S. economic growth has been substantial. That contribution has not been confined to the ITC sector, but can also be seen in the manufacturing, retail, service, and wholesale sectors, all of which have benefited from advances in Internet-enabled computer processing technology and software development. The Internet has contributed to innovation in a wide range of areas, from logistical supply-line optimization to targeted advertisement.

In fact, according to a McKinsey Institute study from 2011, approximately 75 percent of all the economic benefits associated with the Internet accrue to non-ICT industries. The study also estimates that the total international value of goods and services could triple to \$85 trillion over the next decade largely as a result of the proliferation of the Internet and associated communications technologies.<sup>5</sup> It is important to note that the Internet is what economists refer to as a "general purpose technology"—that is, its main value is in its integration with the technologies specific to other industries. The benefits of the ICT market actually accrue most significantly to agriculture, manufacturing, service, wholesale, retail, and other sectors of the economy. In short, U.S. economic development over the past few decades has been driven in no small part by the growth and development of the Internet and related technologies.

If the Internet has been an important source of domestic and international economic growth, then the security protocols that have undergirded the Internet, facilitating its spread, are likely substantial contributors to growth as well.

In addition, the significant NPV associated with an individual firm's adoption of widely available encryption serves to illustrate how advantageous this technology can be. Though the challenges of implementation are indeed very real for many firms, there has nonetheless been increasing use of encryption technologies. Between 2013 and 2014, the use of SSL increased from 2.29 percent to 3.8 percent in North American Internet traffic. In Latin America, the growth was even more dramatic, increasing from 1.8 percent to 10.37 percent during the same time period. Mobile networks are also

---

<sup>4</sup> Dean, David; DiGrande, Sebastian *et al*, "The Internet Economy in the G-20," *BCG Perspectives*, March 19, 2012.

[https://www.bcgperspectives.com/content/articles/media\\_entertainment\\_strategic\\_planning\\_4\\_2\\_trillion\\_opportunity\\_internet\\_economy\\_g20/](https://www.bcgperspectives.com/content/articles/media_entertainment_strategic_planning_4_2_trillion_opportunity_internet_economy_g20/) The total contribution of the Internet to GDP was calculated as 4.7 percent of the given \$14.5 trillion GDP numbers [(0.047)(\$14,500,000,000,000) = \$681,500,000,000].

<sup>5</sup> McKinsey Global Institute, "Internet Matters: The Net's sweeping impact on growth, jobs, and prosperity," *McKinsey & Associates*, May 2011. <https://www.nwoinnovation.ca/upload/documents/mgi-internet-matters-report.pdf>

included in these findings, suggesting that as their popularity increases, so too does the use of encryption.<sup>6</sup>

The difficulty lies in unpacking the relevant data from available sources in order to more narrowly focus on the benefits that encryption specifically contributes to the Internet ecosystem. This job is made all the more difficult by the large number of industries that ICTs touch. To bring some focus and order to the question of encryption's value, the next section will establish a framework for this paper's analysis.

## **METHODOLOGICAL FRAMEWORK**

This paper does not offer a definitive numerical value of encryption's economic value. Such an analysis would require data that does not currently exist. This paper's more modest aim is to draw on the evidence that does currently exist to (a) provide a ballpark estimate of the economic value of encryption and (b) suggest how a more accurate estimate might be achieved. A credible estimate of encryption's benefits to consumers, and to the economy as a whole, will make it easier to defend the integrity of encryption against arguments that it must be weakened in the name of security. The hope is that this paper will show the way toward a better understanding of the role and benefit of encryption in the Internet-age economy.

In order to produce a more rigorous, accurate estimate of the *specific* benefits of software and device encryption technology, more data and research is needed. In particular, a breakdown of specific firm-level data that touches on the amount of time, labor, and resources that goes into the maintenance and implementation of cryptographic systems could help narrow the scope of the question of how valuable encryption is to the ICT industry. A breakdown of similar data in other industries would also help clarify a broader picture of encryption's contribution to economic growth.

For example, the use of software in optimizing logistics plays a significant role in the distribution of goods. A breakdown of a distributor's software platforms into encrypted and non-encrypted categories and the value contribution of each platform to overall revenue would be immensely useful. If breakdowns of this sort were available across most firms in a given industry, a clearer picture of the overall economic value of encrypted systems could be gleaned. Unfortunately, no such data was readily available at the time of this paper's composition.

The evidence presented here is an aggregation of various reports, surveys, and other studies. Based on those numbers, we will attempt to roughly quantify the value of the use of encryption at a broad, macro-economic level, as well as estimating the benefits

---

<sup>6</sup> Sandvine Intelligent Broadband Networks, "Global Internet Phenomena Report: 1H 2014," *Sandvine*, 2014. <https://www.sandvine.com/downloads/general/global-internet-phenomena/2014/1h-2014-global-internet-phenomena-report.pdf>

accruing to individual Internet users. However, this report is primarily intended to spark greater academic interest in what has hitherto been an under-researched issue.

Future work that builds on the following analysis may prove immensely useful in informing and improving the ongoing debates surrounding encryption. Specifying and showcasing the value of encryption in online commerce, banking, and other services will highlight its indispensability to the Internet ecosystem and clarify what's at stake in debates over the integrity and security of encryption.

## **METRICS**

One of the difficulties in determining the value of encryption is the distinction between end-point encryption and encryption of data-in-motion—that is, the difference between the encryption of hardware, such as your computer's hard drive, and the use of software for the encryption of online communications. Hardware device encryption will not be examined in this paper. We'll focus primarily on the software-based encryption used in online transactions. The difficulties involved in estimating the value of software-based encryption are already astoundingly difficult. An examination of the value of device-based encryption would require a paper of its own.

We'll use the following five metrics to evaluate the potential value of encryption. These measures by no means constitute an exhaustive list of the elements that could inform an analysis of the economic benefits of encryption, but they serve as an informed starting point.

**A. Online Banking and Financial Transactions:** Strong encryption protections are important for securing personal financial information. Just as businesses and banks use security, such as armored truck services, for transferring money in the real world, online financial services use encryption to provide security to their clients.

**B. E-Commerce and Online Retail:** Every time individuals purchase goods and services with credit or debit cards, whether in the real world or online, the information transmitted from the point of sale to the financial institution is encrypted. If this were not the case, consumers would be wide open to the theft of their financial information. The same is true with online transactions. There are many elements that go into commercial transactions. This paper focuses exclusively on transactions occurring online and not at point-of-sale terminals in brick-and-mortar locations. However, this is another area that is ripe for an investigation into the benefits of encryption technologies.

**C. ICT Security Revenue, Employment, and Insurance:** Employment levels of ICT security specialists, the revenue ICT firms receive, and the overall cybersecurity insurance market are strong indicators of the value producers place on online

security. Generally speaking, the more a firm invests in security, the more value it places on data protection and securing its systems against cyber attacks.

**D. Research and Development Investment:** The levels of investment in researching and developing online security technologies is suggestive of the value the market places on staying ahead of the technology curve in this space. If the level of R&D increases over time, it is likely that firms see a need to develop better, more advanced security responses to ensure protection against data breaches.

**E. Consumer Surplus:** Although an imperfect measure of the value individuals place on their use of products and services, consumer surplus can nonetheless be used to approximate the quantifiable value placed on ICT security. In particular, the amount of time individuals spend using services that rely on encryption sheds light on the value they place on these services.

These metrics provide a suggestive indication of the value associated with encryption's proliferation and use. However, while these measures afford a general sense of how valuable ICT security is in the modern age, the specific numbers associated with these analyses are aggregates of various reports and studies that do not focus on encryption specifically.

## **ASSESSING THE BENEFITS**

### **A. Online Banking and Financial Transactions**

As far back as 1995, the benefits of encryption were well established in the banking industry.<sup>7</sup> Indeed, since the early 1970s, the financial community has recognized the value of cryptography as a means of securing fund transfers for clients. In the years since the Internet's emergence, the value of secure online fund transfers for individuals has also taken off.

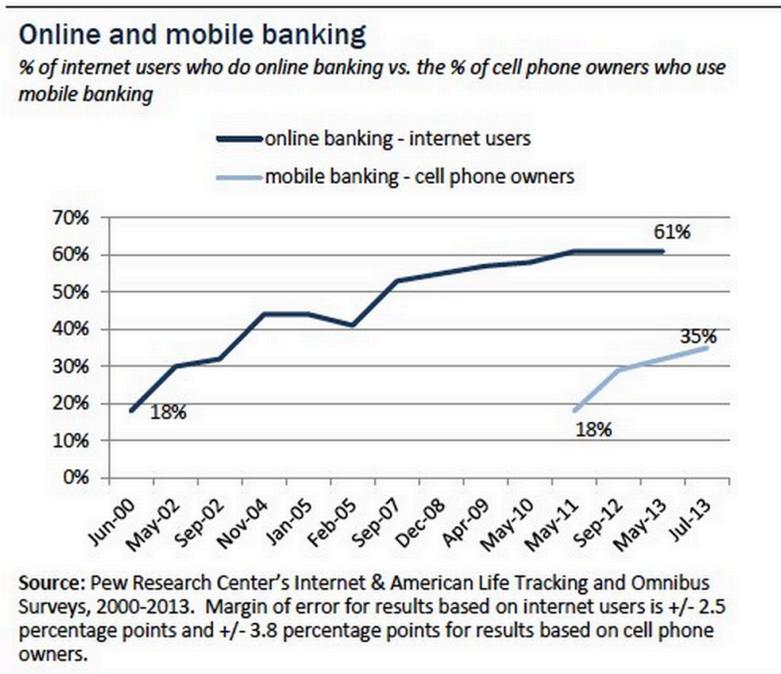
As of 2013, approximately 30 million households reported using online banking through mobile devices—an increase of 21 percent from 2012. The overwhelming majority of those using smartphones and other mobile devices as a platform for online banking were younger people, classified as Generation X (37 percent) and Generation Y (57 percent). Similarly, more and more individuals are engaging in online financial service usage via phone and tablet apps, as opposed to mobile browsers. A Fiserv report notes that the vast majority of individuals it surveyed use online, app-based mobile banking to view account balances, transfer funds, and view monthly statements “with 70 percent

---

<sup>7</sup> U.S. Department of Commerce and the National Security Agency, “A Study of the International Market for Computer Software with Encryption,” *Interagency Working Group on Encryption and Telecommunications Policy*, 1995. [https://www.bis.doc.gov/index.php/forms-documents/doc\\_view/24-a-study-of-the-international-market-for-computer-software-with-encryption-nsa-1995](https://www.bis.doc.gov/index.php/forms-documents/doc_view/24-a-study-of-the-international-market-for-computer-software-with-encryption-nsa-1995).

citing 24/7 access to account balances and 64 percent citing the ability to access a bank account from anywhere” as the primary benefits associated with these services.<sup>8</sup>

As the Pew Research Center has noted, over 60 percent of Internet users bank online, and 35 percent of smartphone owners bank using mobile devices. Those numbers have risen sharply over the years. Internet users engaging in online banking rose from 18 percent in 2000 to approximately 61 percent by June 2013—a 30 percent increase. Even more notable has been the meteoric rise of online banking via mobile devices, which stood at 18 percent of cell phone users in 2011 and rose to 35 percent just two years later in 2013—a 50 percent increase in user adoption over just two years.<sup>9</sup>



It is also worth noting that online users tend to feel more secure on financial institution websites than elsewhere on the Internet. As a comScore survey from 2011 points out, “customers still reported feeling more secure on their [financial institution’s] website than on the Internet as a whole. General sentiment indicated that security had either remained the same or improved. Only 6 percent of customers felt less secure on their

<sup>8</sup> Fiserv Consumer Trends Survey, “Digital Banking Shifts Compel Financial Institutions to Think Holistically about Online, Mobile and Tablet Channels,” Fiserv, 2013. [https://www.fiserv.com/resources/100-14-20222-COL\\_2\\_5\\_RP\\_ConsumerTrendsSurvey2013\\_v05cs\\_1407.pdf](https://www.fiserv.com/resources/100-14-20222-COL_2_5_RP_ConsumerTrendsSurvey2013_v05cs_1407.pdf). As the Fiserv report notes, “More consumers are accessing mobile banking using an app instead of browser or test ... this is likely due to the increased ownership of smartphones ... as well as the enhanced experience offered by apps, which enable capabilities such as remote deposit of checks using the smartphone camera.”

<sup>9</sup> Fox, Susanna, “51% of U.S. Adults Bank Online,” *Pew Research Center*, Aug. 7, 2013. <http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/>

[financial institution's] site in 2011 compared to last year, but that number was lower than the 12 percent who felt less secure on the Internet as a whole."<sup>10</sup> Essentially, customers trust their bank's website when engaging in financial transactions online.

According to a McKinsey and Company report from 2012,

Consumer acceptance of connecting to banking services via a social media platform has evolved over the last few years. In 2008, a survey of 400 Facebook users found that only 14 percent were receptive to the idea of banking on a social platform; by 2012, the share had risen to 24 percent. According to comScore, the number of customers visiting the top ten online banking sites increased from approximately 40 million people in 2006 to more than 58 million in 2010. Nearly 60 percent of US Internet users visited at least one of the top 20 financial institution Web sites every quarter in 2010.<sup>11</sup>

Unfortunately, this comfort is not expressed in perceptions related to mobile devices. The study goes on to point out that, in addition to other barriers to smartphone adoption, "negative perceptions around the security of account servicing via mobile devices," remains high on the list.<sup>12</sup>

The need for consumers to be comfortable in the knowledge that their financial transactions are secure is increasingly important for younger users. As a study from Mahmood Hussain and Clarice Wong points out: "Generation Y members ... prefer online over mobile banking; when banking online, they only pay bills, view banking statements and perform money transfers." Those on the older end of the Generation Y demographic (late-20s to early 30-s) "prefer to bank online or with their phone, especially if they are heavy users of the Internet."<sup>13</sup>

Perhaps even more impressive than the online banking figures is the *trillions* of dollars involved in online financial transactions processed every year. In 2001, Fedwire and the Clearing House Interbank Payment System processed over 350,000 messages daily, with daily valuation totaling anywhere between \$1-2 trillion. As of 2010, the total number of electronic payments was 84.5 billion, with a total value of over \$40 trillion.<sup>14</sup>

---

<sup>10</sup> *2011 State of Online and Mobile Banking*, comScore Financial Services report, February 2012

<sup>11</sup> McKinsey Global Institute, "The Social Economy: Unlocking Value and Productivity through Social Technologies," *McKinsey & Company*, Nov. 2012.

[https://www.mckinsey.com/~media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/The%20social%20economy/MGI\\_The\\_Social\\_Economy\\_Consumer\\_financial\\_services.ashx](https://www.mckinsey.com/~media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/The%20social%20economy/MGI_The_Social_Economy_Consumer_financial_services.ashx).

<sup>12</sup> Nathan Frederiksen and Sarah Lenart, *2011 State of Online and Mobile Banking*, comScore Financial Services report, February 2012.

<sup>13</sup> Mahmood Hussain and Clarice Wong, *The Online Banking Behavior of Generation Y*, International Business and Economy Conference, January 2015.

<sup>14</sup> Financial Services Policy Committee, "Federal Reserve Payments Study Provides Details on Increasing Role of Electronic Payments," *Federal Reserve System*, April 5, 2011.

A Federal Reserve Payments Study from 2013 further found that although paper checks continue “to persist as a significant portion of noncash payments ... interbank processing and clearing of these checks are virtually all electronic.”<sup>15</sup> Without strong encryption protecting these transfers, the number of fraudulent transactions would undoubtedly be significantly higher. Data breaches for financial institutions are among the primary motivations for the industry’s heavy investment in encryption.

A 2014 study from the Ponemon Institute reports that almost half of 4,800 IT managers interviewed globally “said that the main reason they invested in encryption was that it could lessen the impact of [data] breaches.”<sup>16</sup> Additionally, the study notes that the use of encryption has doubled, with 30 percent of organizations now utilizing it to some extent. Financial institutions lead the way, with 43 percent incorporating the use of encrypted communications. One of the most notable insights was the recognition that encryption use should be much higher than it is. The main barrier to more widespread adoption is the complexity of encryption key management, which has led many firms to conclude that implementation could be expensive. However, Forrester Consulting’s report clearly shows the benefits of encrypted systems far outweigh the costs.<sup>17</sup>

### **Analysis: Online Banking and Financial Transactions**

Encryption’s contribution to the rise of online banking is an under-researched area. More data is needed for a more detailed analysis, but the available information suggests that the value of online banking is substantial. The 50 percent increase in mobile online banking over a mere two years (2011 to 2013) shows that consumers value these services. A feeling of security is important for the increasing user adoption of mobile banking, as evidenced by the concerns users express over uncertainty surrounding account servicing on mobile devices. Weakening the cryptographic protocols will certainly not ameliorate those concerns. When it comes to the online security of personal finances, consumers—especially younger consumers—take note.

And, of course, the astronomic growth of electronic interbank payment processing—from a daily valuation between \$1-2 trillion in 2001 to over \$40 trillion as of 2010—would likely have been impossible had banking institutions been significantly uncertain of the security protocols encrypting transactional data. It is a safe assumption that had strong

---

[https://www.frbervices.org/files/communications/pdf/press/040111\\_2010\\_payments\\_study\\_press\\_release.pdf](https://www.frbervices.org/files/communications/pdf/press/040111_2010_payments_study_press_release.pdf)

<sup>15</sup> Gerdes, Geoffrey *et al*, “The 2013 Federal Reserve Payments Study,” *Federal Reserve System*, Dec. 19, 2013.

[https://www.frbervices.org/files/communications/pdf/research/2013\\_payments\\_study\\_summary.pdf](https://www.frbervices.org/files/communications/pdf/research/2013_payments_study_summary.pdf)

<sup>16</sup> Dunn, John E., “Data breaches drive growth in use of encryption, study finds,” *Tech World*, Feb. 11, 2014. <http://www.techworld.com/news/security/data-breaches-drive-growth-in-use-of-encryption-global-study-finds-3501515/>

<sup>17</sup> *Ibid.*

encryption not been readily available, or had been weakened by politically mandated security vulnerabilities, this growth would have been significantly stunted.

It is important to recognize that the security of consumers and institutions are tightly related. A lack of strong consumer-end security, even when coupled with strong institutional security, can lead users to worry and forego the efficiencies of online banking. The reverse is also true. The full benefit of encryption comes from strong security at every step of the transaction.

## **B. e-Commerce and Online Retail**

In 1994, total online business transactions were estimated at around \$100 million. By 2000 the U.S. Department of Commerce predicted a 3,000-fold increase in the e-commerce sector to \$300 billion.<sup>18</sup> According to a 2000 Brookings Report, the e-Commerce economy was estimated at somewhere between \$100-200 billion.<sup>19</sup> That market was estimated to have grown to \$250 billion by 2009.<sup>20</sup> In the second quarter of 2015 alone, e-Commerce was estimated to be almost \$84 billion, accounting for 7.2 percent of total retail sales—an increase of over 14 percent from the previous year.<sup>21</sup>

The growth of e-commerce is not new. As the following graph shows, online retail commerce has been growing at a steady rate ever since the late 1990s.

---

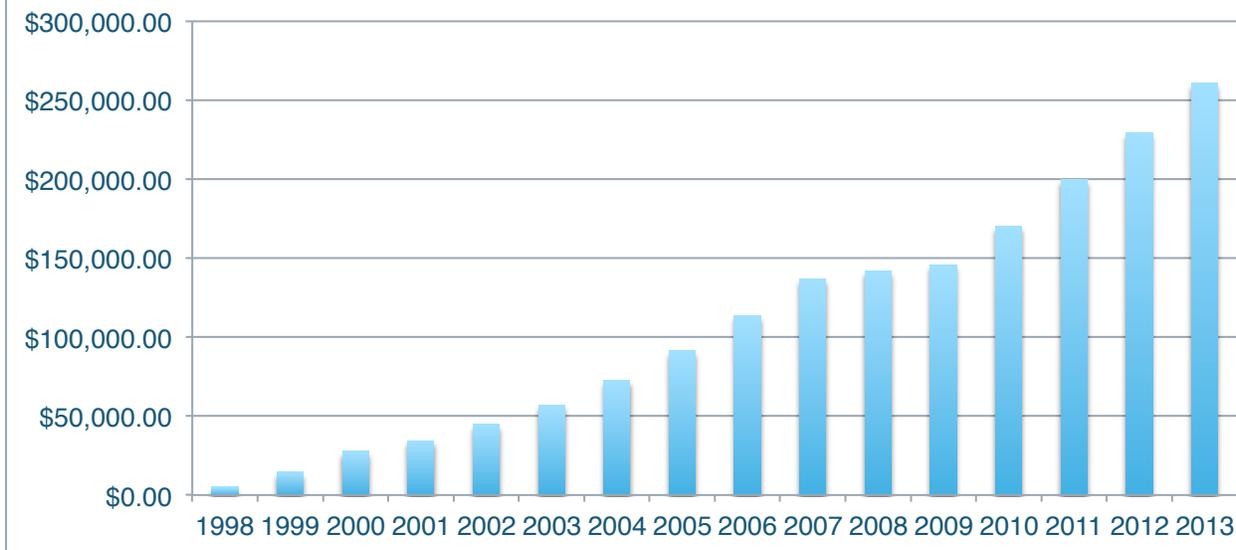
<sup>18</sup> U.S. Department of Commerce and the National Security Agency, “A Study of the International Market for Computer Software with Encryption,” *Interagency Working Group on Encryption and Telecommunications Policy*, 1995. [https://www.bis.doc.gov/index.php/forms-documents/doc\\_view/24-a-study-of-the-international-market-for-computer-software-with-encryption-nsa-1995](https://www.bis.doc.gov/index.php/forms-documents/doc_view/24-a-study-of-the-international-market-for-computer-software-with-encryption-nsa-1995).

<sup>19</sup> Alice Rivlin and Robert Litan, “The Economy and the Internet: What Lies Ahead?” *The Brookings Institution*, Dec. 2000. <http://www.brookings.edu/research/papers/2001/12/technology-litan>

<sup>20</sup> McKinsey Global Institute, “Internet Matters: The Net’s sweeping impact on growth, jobs, and prosperity,” *McKinsey & Associates*, May 2011. <https://www.nwoinnovation.ca/upload/documents/mgi-internet-matters-report.pdf>

<sup>21</sup> Rebecca DeNale, Xijian Liu, and Deanna Weidenhamer, “U.S. Census Bureau News,” *U.S. Department of Commerce*, Aug. 17, 2015. [https://www.census.gov/retail/mrts/www/data/pdf/ec\\_current.pdf](https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf)

## U.S. e-Commerce Retail Sales (millions of \$) 1998-2013



Source: Census Data from U.S. Annual Retail Trade Survey (1998-2013)

In 2013, the value of e-commerce shipments for U.S. manufacturing firms was \$3.3 trillion; the value of all shipments was \$5.8 trillion. That means online purchases were responsible for almost 60 percent of the value of total manufacturing shipments in 2013. Wholesale e-commerce accounted for 26.5 percent of the total sales.<sup>22</sup> Online purchases have increased steadily over the past 15 years as a percentage of total retail sales, as well as in absolute terms, with no end to the growth in sight. These numbers and trends suggest the increasing importance of e-commerce to various traditional industries, as well as the increased value consumers are placing on these online services.

### Analysis: e-Commerce and Online Retail

With a 2009 market valuation of over \$250 billion, e-commerce transactions, though still a relatively small proportion of total retail sales, have increased substantially since 1998. In manufacturing, however, approximately 60 percent of total shipments in 2013 resulted from online purchases, totaling \$3.3 trillion. Nowhere is the value of encryption, especially the use of SSL and TLS website security protocols, more apparent than with online merchants, such as Amazon.com. Without a secure encryption protocol to keep

<sup>22</sup> *E-Stats 2013: Measuring the Electronic Economy*, 28 May 2015; In all four of the sectors surveyed (manufacturing, wholesale, service, and retail), the 2012 estimates of growth all ended up being underestimated. To wit, in 2012 manufacturing e-commerce shipments were estimated to be \$3 trillion by 2013. Instead they were \$3.3 trillion – a difference of 11.1 percent.

customer data secure when in-transit for payment processing, such online commerce would be far less trusted and far less used.

Given the necessity of secure payment transactions when purchasing via electronic means, the value of encryption is certainly much greater than zero, but less than the total value of e-commerce in a given year. The trouble lies in pinpointing where it falls along that range. More data is needed to home in on a precise number, but it is safe to say that the growth of e-commerce, as well as total online sales, would have been greatly diminished without the use of encryption.

### **C. ICT Security Revenue, Employment, and Insurance**

One broad measure of encryption's importance to the economy is the scale and scope of the industry providing cryptographic products and services. Unfortunately, these types of products and services are only a sub-component of the broader market for ICT security. As such, there is currently extremely limited time-series data on the size of the domestic and international markets for cryptographic products and services. However, we can make some broad assumptions as to the value placed on ICT security in general, which is at least suggestive of the value consumers and producers place on encryption.

For example, the rapid and expansive growth of revenues for top cybersecurity firms can be seen as a rough proxy for the value of encryption. Online ICT security is a large and growing industry.<sup>23</sup> The top three cybersecurity firms in 2014, in terms of total revenue, were Kaspersky Labs, Palo Alto Networks, and FireEye. They took in \$711 million, \$598.2 million, and \$425.7 million, respectively. From 1996 to 1997, the worldwide Internet security software market grew 67 percent, from \$1.2 billion to \$2 billion. The expected growth of this market for 1998 was \$3.1 billion, \$4.2 billion for 1999, and \$7.4 billion for 2002.<sup>24</sup> As of 2015, the total size of the global cybersecurity market had exploded to over \$100 billion, with an estimated growth to \$170 billion by 2020.<sup>25</sup> The growth of cybersecurity firm revenue and the increasing global market value of the online security sector are representative of the growing importance that firms are placing on online security.

---

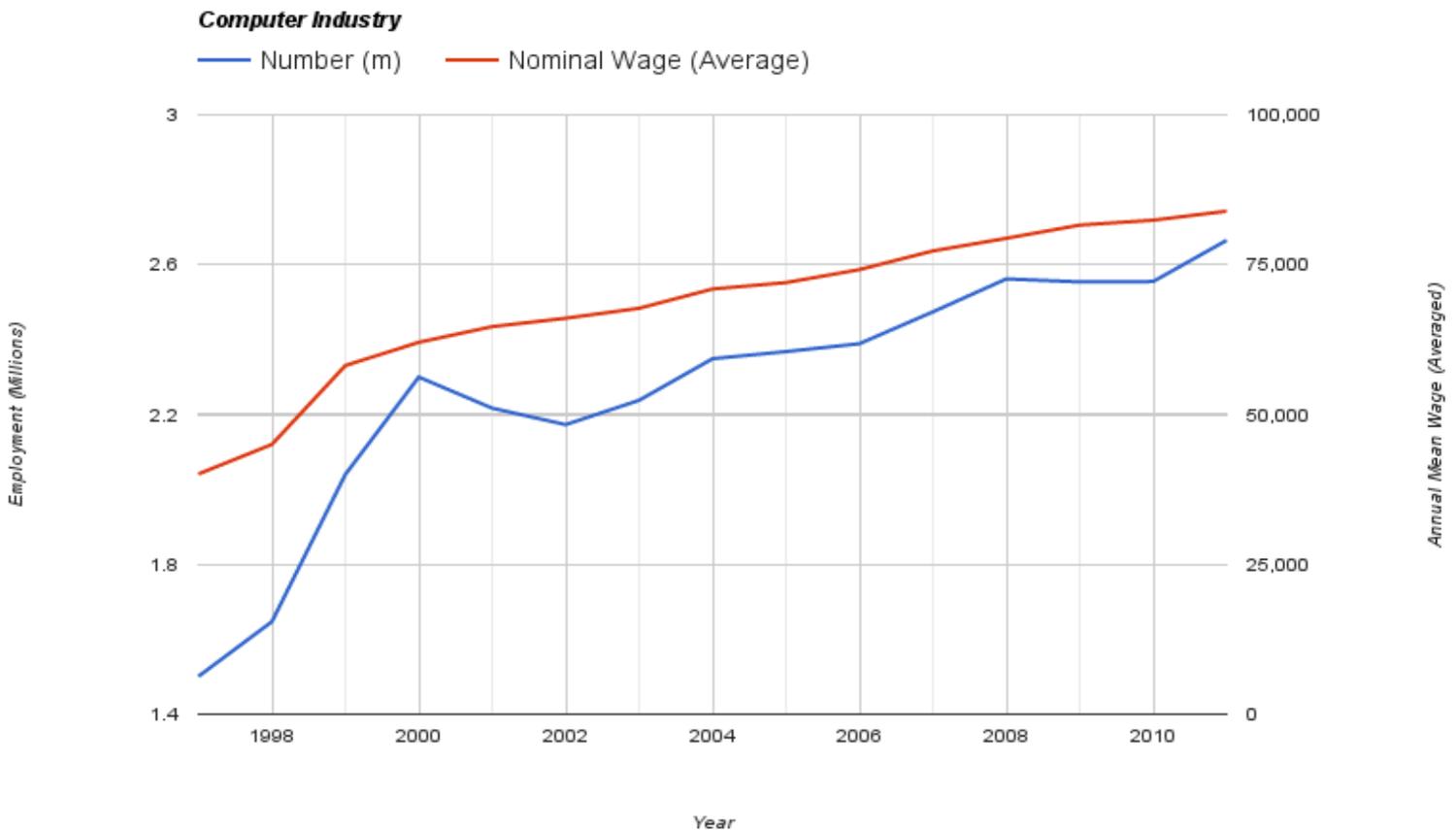
<sup>23</sup> "Kaspersky Lab Overview," <http://www.kaspersky.com/about>; "Palo Alto Networks Reports Fiscal Fourth Quarter and Fiscal Year 2014 Financial Results," <http://investors.paloaltonetworks.com/phoenix.zhtml?c=251350&p=irol-newsArticle&id=1965398>; "FireEye Reports Record Financial Results for Fourth Quarter and Fiscal Year 2014," <http://investors.fireeye.com/releasedetail.cfm?ReleaseID=895954>

<sup>24</sup> David Leech, Michael Chinworth, *The Economic Impacts of NIST's Data Encryption Standard (DES) Program*, Oct. 2001.

<sup>25</sup> "Cybersecurity Market Report," *Cybersecurity Ventures*, <http://cybersecurityventures.com/cybersecurity-market-report/>

Employment trends in the ICT security industry also suggest the increasing importance and value of its services. In 2000, the Bureau of Labor Statistics (BLS) did not have a classification for information security analysts.<sup>26</sup> By 2010, information security analysts were included in a category together with web developers and computer network architects.<sup>27</sup> By 2014, the number of information security analysts had grown enough to merit a completely independent category.<sup>28</sup> In 1997, the title “information security analyst” did not exist. By 2014, over 80,000 information security analysts were employed by firms.<sup>29</sup>

As the accompanying graph shows, employment in the computer industry has changed substantially since 1997.<sup>30</sup> The industry grew from a little over 2 million to just under 4 million in the 15 years between 1997 and 2012.



<sup>26</sup> “List of SOC Occupations,” 2001 [http://www.bls.gov/oes/2000/oes\\_stru.htm#15-0000](http://www.bls.gov/oes/2000/oes_stru.htm#15-0000)

<sup>27</sup> “Occupational Employment and Wages, May 2010” <http://www.bls.gov/oes/2010/may/oes151179.htm>

<sup>28</sup> “Occupational Employment and Wages, May 2014.” <http://www.bls.gov/oes/current/oes151122.htm>

<sup>29</sup> Ibid.

<sup>30</sup> Desilver, Drew, “How U.S. tech-sector jobs have grown, changed in 15 years,” *Pew Research Center*, March 12, 2014. <http://www.pewresearch.org/fact-tank/2014/03/12/how-u-s-tech-sector-jobs-have-grown-changed-in-15-years/>.

It is also worth noting the value and growth of the cybersecurity insurance market. In 1999, for the first time ever, the total cost of data breaches topped \$1 billion. Over time, the market for insurance against cyber-attacks has grown and, as of 2015, according to Markets & Markets, the size of the global cybersecurity market was \$106.32 billion.<sup>31</sup> This number is expected to grow in coming years, especially as it becomes more and more apparent that there is no silver bullet solution for absolute online security.

The International Data Corporation (IDC) predicts that by the end of this year, approximately 20 percent of all proprietary data held in the cloud will be encrypted; by 2018 that percentage is projected to rise to 80 percent.<sup>32</sup> By 2019, the software market for encryption is forecasted to be valued at over \$4.8 billion.<sup>33</sup> Such growth and market valuation provides insight into the value that producers place on the need to secure customer data.

### **Analysis: ICT Security Revenue, Employment, and Insurance**

While these numbers certainly suggest there has been, and continues to be, rising demand for employment in the ICT security profession, they are insufficient as a measure of the demand for encryption services. After all, the ICT security profession deals not only in end-point and software encryption, but also includes systems penetration experts, database security, and network security, to say nothing of the myriad other activities often included under the rubric of ICT security. As such, the increase in employment for this particular Occupational Employment Statistics (OES) classification is by itself unlikely to tell the full story of the rise in importance of encryption.

One problem with this data is that it fails to track self-employed individuals. Without data covering the entire ICT security labor market, estimates of total employment in the sector are likely conservative. Millennials are especially likely to engage in part-time and contract work, compared to older workers, which is another reason to suspect that official data understate the number of people working in ICT security.

Spotty data notwithstanding, increases in ICT security-firm revenue, growing employment numbers for ICT security professionals, and growth in the cybersecurity insurance market together speak to the increasing economic importance of encryption. When coupled with investments in R&D and the growth of ICT security product patent

---

<sup>31</sup> MarketsAndMarkets, "Cyber Security Market worth \$170.21 Billion by 2020."  
<http://www.marketsandmarkets.com/PressReleases/cyber-security.asp>

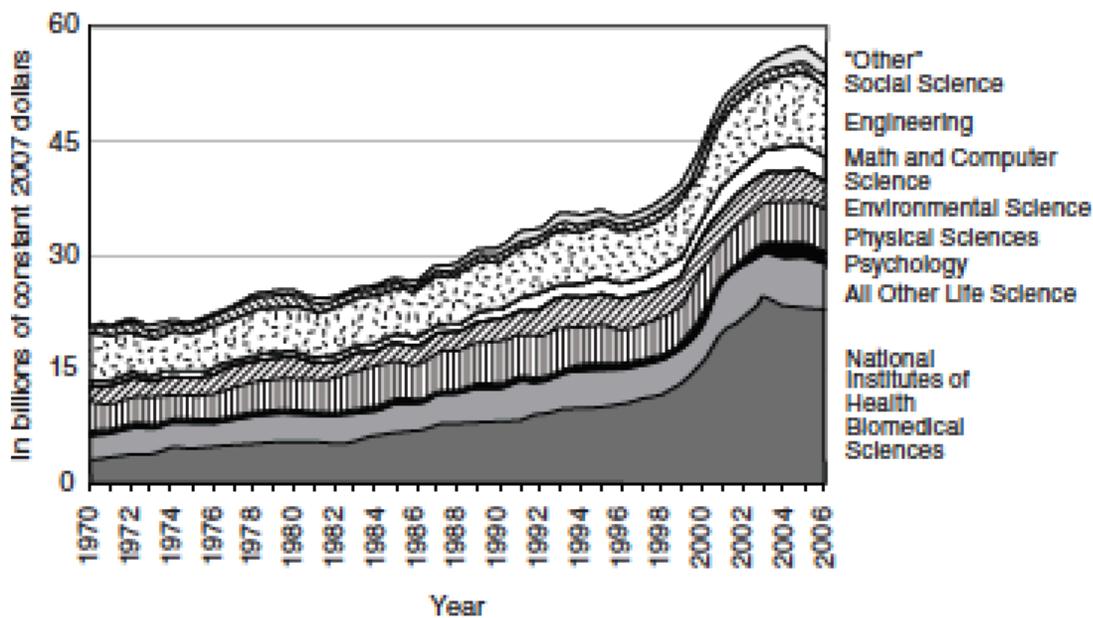
<sup>32</sup> IDC, "IDC Reveals Worldwide Security Predictions for 2015," Dec. 11, 2014.  
<http://www.idc.com/getdoc.jsp?containerId=prUS25333114>

<sup>33</sup> Cybersecurity Ventures, "Cybersecurity Market Report," Q3, 2015.  
<http://cybersecurityventures.com/cybersecurity-market-report/>

applications—all assessed in the next section—the argument for encryption’s increasingly vital economic role becomes even stronger.

#### D. Research and Development Investment

As can be seen in the graph below<sup>34</sup>, federal funding for math and computer science research and development is dwarfed by outlays for basic and applied research. The late 1990s and early 2000s saw a large rise in overall federal funding for basic and applied research. Of course, this by itself is not indicative of greater investment in encryption and cybersecurity technologies. Rather, these are components of the overall growth in R&D spending that, unfortunately, are not specifically accounted for in a more detailed breakdown of science and technology expenditures.

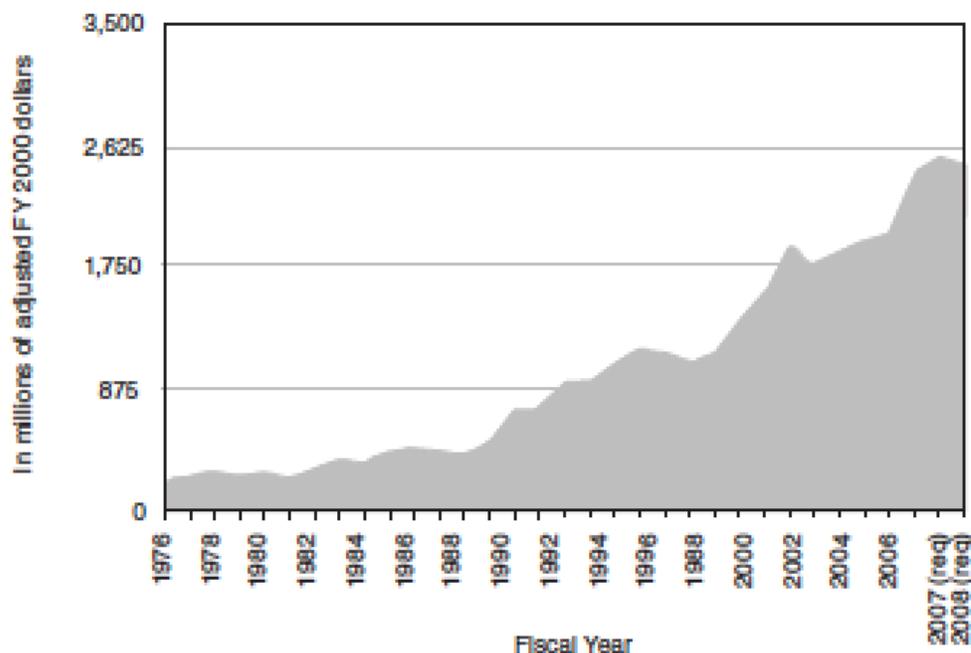


Looking to the next graph<sup>35</sup>, which depicts the trend in ICT federal funding, while not exclusively focused on encryption, can serve as a useful proxy variable for investment in online and software protection technologies. The growth in federal research and development also reveals the increased importance that the federal government has placed on this space. The dramatic increase in funding in the late 1990s and early

<sup>34</sup> *Assessing the Impacts of Changes in the Information Technology R&D Ecosystem: Retaining Leadership in an Increasingly Global Environment*, 2009 National Research Council of the National Academies Report

<sup>35</sup> *Assessing the Impacts of Changes in the Information Technology R&D Ecosystem: Retaining Leadership in an Increasingly Global Environment*, 2009 National Research Council of the National Academies Report

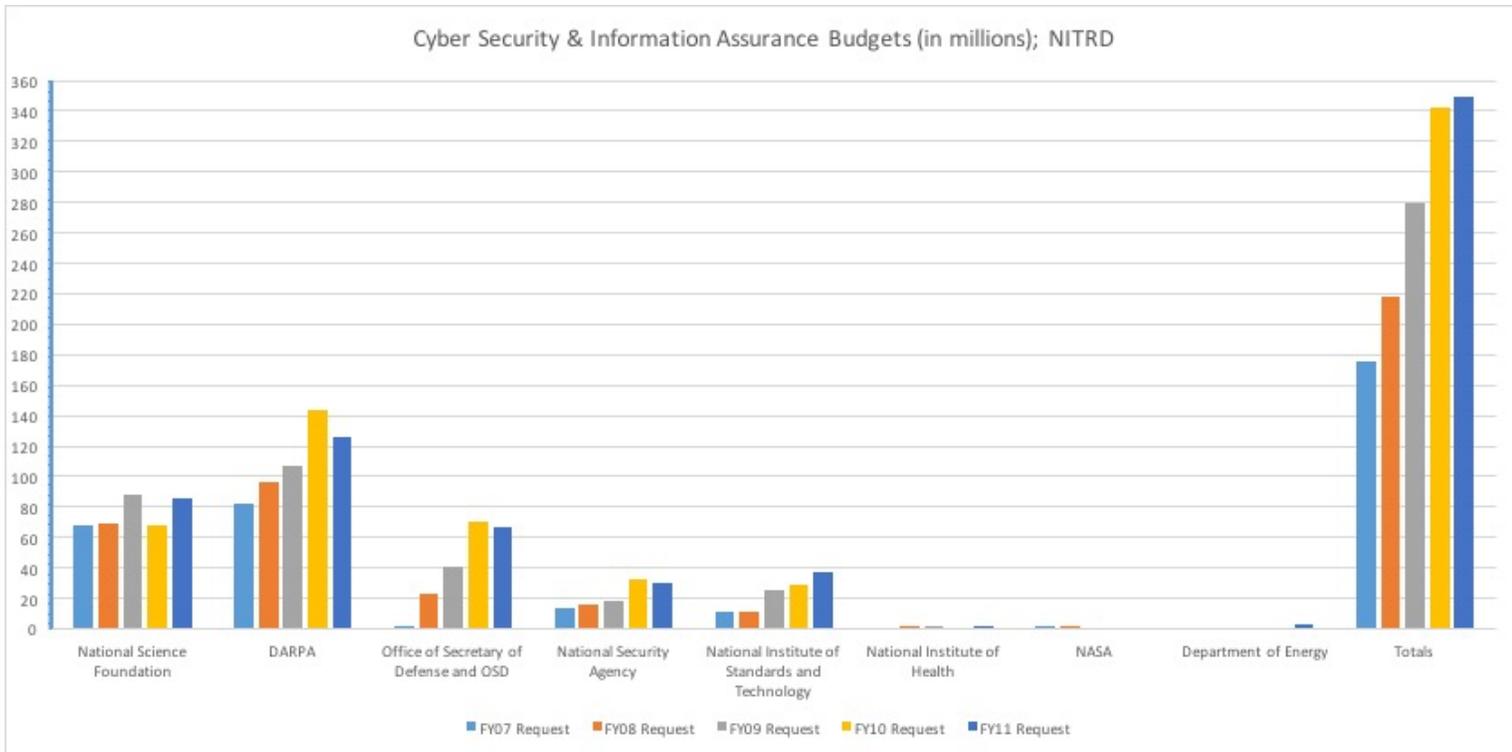
2000s is particularly interesting to note, as it corresponds with the mass adoption of the commercial Internet.



Although specific R&D funding for online security is difficult to tease out, the requests made by federal agencies for funding related to mathematics and computer science suggests that agencies think it is important. The graph below gives a breakdown of funding requests by various federal agencies, courtesy of the Networking and Information Technology Research and Development (NITRD) Program.<sup>36</sup> Funding requests differ year-by-year, but the overall breakdown of requests across federal agencies shows an ever-increasing desire for funds to secure online operations and data. The dataset here only assesses requests between 2006 and 2011, but if the other metrics examined in this report are any indication, we would expect funding requests to be even higher today than they were in 2011.

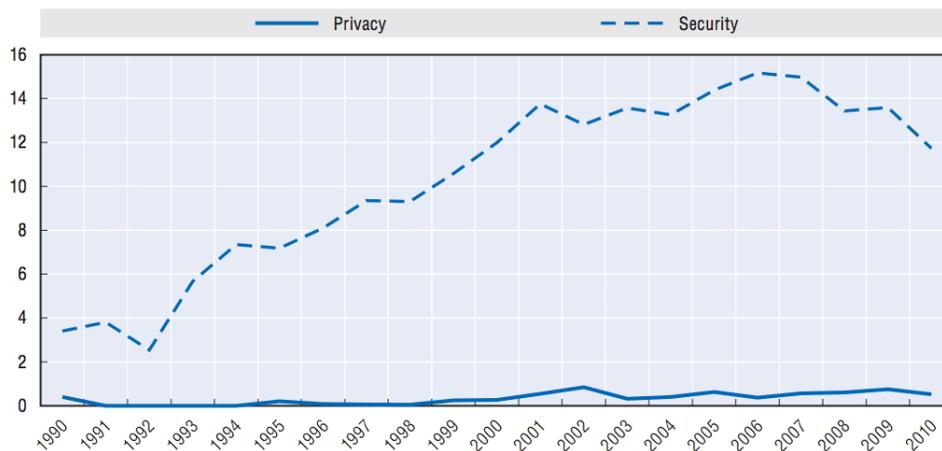
The logic of using budget requests rather actual budgets is that requests are better indicators of the agencies' judgments about the value of investing in security. Actual budgets, given the political nature of appropriations—not to mention the fact that some of the budget may be awarded to the agency as a whole and then internally earmarked for cybersecurity and information assurance—are less likely to reflect the agencies' sense of their own needs.

<sup>36</sup> Carl Landwehr, *History of US Government Investments in Cybersecurity Research: A Personal Perspective*, Institute for Systems Research, University of Maryland – College Park, 2010, <http://www.landwehr.org/2010-landwehr-sp10-final.pdf>.



The growth of applications for ICT security patents can also serve as a telling indicator of the increasing importance of ICT security for individual firms. Although patents by themselves are not necessarily indicative of growing value in a given market, when coupled with the other metrics, a clear trend emerges. As indicated in the graph below, the number of patent applications for information security products grew from less than 3 percent in 1992 to almost 14 percent by 2002 (relative to other applications). Although this number has dropped off in recent years, the sevenfold increase in patent applications over this time period—the same period during which the Internet’s explosive growth began to take off—suggests the increasing importance of this emerging market.

Figure 7.4. **Relative number of patent applications in information security and privacy filed under PCT, 1990-2010**  
Per thousand ICT patent applications



Notes: Security-related applications are identified with keywords such as “recovery” “virus” and “spyware” (“security” and “computer”). Privacy-related applications are identified with keywords such as “anonymity”, “identity” and “privacy”.  
Source: OECD Patent Database, June 2012.

StatLink  <http://dx.doi.org/10.1787/888932694633>

In each of these cases, a precipitous growth period is correlated with the emergence of the commercialized Internet. Growth of R&D funding for ICTs and growth in the number of patent applications for ICT security steadily increased during periods of growth in Internet adoption. Together with the growth trends in ICT security employment and firm revenue, in the cybersecurity insurance market, in e-Commerce sales, and in online financial transactions, these trends in R&D funding and patent application add to the emerging picture of the value of encryption.

### **Analysis: Research and Development Investment**

Whether and how research and development contributes to the growth and acceptance of new technologies raises the question of the chicken and the egg: which came first? Did R&D spur the rise of the Internet and advancements in ICT security technology, or was it the growth of these technologies that spurred greater investment in R&D? Because there is no easy way to settle the question, the trend in R&D investment over time should be taken as merely suggestive.

However, the numbers provided above are nonetheless indicative of increasing investment in ICT security products and services. Coupled with the overall rise in ICT security product patents, the reasonable conclusion is that the market for online security tools is increasing. This would make sense, especially when taken together with the increase in ICT security employment, growing revenues of industry firms, and the increasing market valuation of global cybersecurity insurance.

## E. Consumer Surplus

Attempting to sketch out a picture of the economic value derived from the availability and ubiquitous proliferation of encryption protocols is no easy task. Attempting to quantify individual consumer surplus is no easier. Consumer surplus—usually defined as the difference between what a consumer is willing to pay for a good or service and what they actually do pay—is a way to measure the contribution an episode of consumption makes to an individual’s well-being. It’s a sometimes controversial measure, especially when it is used in attempts to capture the value that individuals place on intangible things, such as privacy and security.<sup>37</sup> Of course, the value of encryption to individuals is largely a matter of the value they place on privacy and security. So estimating the consumer surplus of encryption is a difficult job.

Nevertheless, a recent behavioral economics study does help us to see the value that one might attach to online privacy and security. If given the option, and no “free” encryption is available, a 2005 study suggests that a significant majority of users will pay some price for minimizing risk against identity theft. This could include paying for insurance, encrypting data, or hiring a “detective” to validate the authenticity of a website receiving the user’s information. The study concluded: “The results of ... preliminary experiments indicate that Internet users are willing to pay hefty sums to increase security.”<sup>38</sup>

Econometric estimates of the consumer surplus deriving from Internet use supports this conclusion. A McKinsey Global Institute report from 2011 estimated the total global consumer surplus accruing from the Internet to be over \$130 billion. Importantly, the report notes that a little over half (52 percent) of this surplus was derived from communications and search services that tend to rely on encryption. E-mail, online search, social networks, and instant messaging were estimated to generate \$4.28, \$4.28, \$2.94, and \$2.81 worth of consumer surplus per month, respectively.<sup>39</sup>

Therefore, based on this study, approximately \$67.7 billion worth of consumer surplus accrued to individuals as a result of the use of services that rely heavily on encryption. If we take into account the fact that the total number of global Internet users numbered almost 2.3 billion in 2011, it follows that individuals gained approximately \$29.40 worth

---

<sup>37</sup> Greenstein, Shane, “Measuring Consumer Surplus Online,” *The Economist: Free Exchange Economics* March 11, 2013. <http://www.economist.com/blogs/freeexchange/2013/03/technology-2>

<sup>38</sup> David Baumer, Julia B. Earp, and J.C. Poindexter, *Quantifying Privacy Choices with Experimental Economics*, Workshop on the Economics of Information Security, 2005.

<sup>39</sup> Bughin, Jacques, “The Web’s €100 billion surplus,” *McKinsey Quarterly*, Jan. 2011. [http://www.mckinsey.com/insights/media\\_entertainment/the\\_webs\\_and\\_8364100\\_billion\\_surplus](http://www.mckinsey.com/insights/media_entertainment/the_webs_and_8364100_billion_surplus). (The original assessment of consumer surplus was evaluated in Euros. For the purpose of conversion to USD, the 2011 exchange rate for dollars to Euros (\$1 for every 0.748 Euros) provided by the IRS website was used.)

of consumer surplus annually as a result of the use of services that utilized some form of encryption.<sup>40</sup>

Erik Brynjolfsson and Joo Hee Oh of the Massachusetts Institute of Technology have argued that, “between 2002 and 2011, the amount of leisure time Americans spent on the internet rose from 3 to 5.8 hours per week.” That 2.8 hour growth, according to the authors, reflected a growing accumulation of consumer surplus from Internet usage, “which they value at \$564 billion in 2011, or \$2,600 per user.”<sup>41</sup> Similarly, Shane Greenstein and Ryan McDevitt, economists at Harvard and Duke, calculated potential consumer surplus from Internet usage based on the real price of broadband access as calculated in 1999 and 2006. They concluded, “by 2006 broadband was generating \$39 billion in revenue and \$5 billion-\$7 billion in consumer surplus a year.”<sup>42</sup>

### **Analysis: Consumer Surplus**

Clearly, consumers value encryption. Using the McKinsey study previously mentioned, a rough estimate of the annual consumer surplus resulting from the use of ICT services employing encryption was \$29.40 per user. However, this number could be deceptively low. The issue of consumer surplus is a murky measure of individual welfare. With regards to the previous figure, *The Economist* notes that Brynjolfsson’s and Oh’s numbers “probably understate [consumer surplus].”

The authors’ calculations assume Internet access meant the same thing in 2006 as it did in 1999. But the advent of new services such as Google and Facebook meant Internet access in 2006 was worth much more than in 1999. So the surplus would have been bigger, too.<sup>43</sup>

The fundamental problem in attempting to tease out the proportion of consumer surplus that could be attributable to encryption is the sheer complexity of the Internet ecosystem. The value of encryption today is likely more than it was even just 10 years ago, given the increased network effects and innovative services that have developed over time. As more of our lives move online, the value we acquire from the use of ICTs

---

<sup>40</sup> This calculation was achieved by merely dividing the total number of global Internet users in 2011 by the total global consumer surplus. <http://www.internetlivestats.com/internet-users/#trend>

<sup>41</sup> *The Economist*, “Net Benefits: How to Quantify the gains that the Internet has brought to consumers,” March 7, 2013. <http://www.economist.com/news/finance-and-economics/21573091-how-quantify-gains-internet-has-brought-consumers-net-benefits>

<sup>42</sup> *The Economist*, “New Benefits: How to quantify the gains that the Internet has brought to consumers,” March 7, 2014. <http://www.economist.com/news/finance-and-economics/21573091-how-quantify-gains-internet-has-brought-consumers-net-benefits>.

<sup>43</sup> *The Economist*, “Net Benefits: How to quantify the gains that the Internet has brought to consumers,” March 7, 2013. <http://www.economist.com/news/finance-and-economics/21573091-how-quantify-gains-internet-has-brought-consumers-net-benefits>.

and security technologies like encryption increases. Quantifying that increase in consumer surplus, however, is difficult.

## CONCLUSION

Innovation never occurs in a vacuum; it is in part the byproduct of the institutional environment produced by policymakers. It is imperative that regulators and legislators remain humble in the face technological change and progress. They must recognize that attempts to regulate vital elements of the Internet ecosystem are likely to lead to a series of unintended consequences. Until we have a more accurate picture of the specific economic benefits of encryption, government officials would be well advised to avoid mandates for backdoor access—that is, to avoid mandating security vulnerabilities—in this technology. Given the trillions of dollars of daily electronic financial transactions that rely on encryption, as well as the broader economic impact of its use by consumers and producers, any mandate that would reduce online security risks doing significant damage to the modern economy.

The physical world is increasingly wired to the Internet. Water treatment plants and automobiles now constantly exchange information over the Internet, creating whole new concerns about the security of networks. Encryption will only become more important in the coming years as more and more “things” become interconnected.

This paper has journeyed into the hitherto under-researched economic benefits calculations associated with encryption. While the data is incomplete and difficult to evaluate, it is clear that there are immense, semi-quantifiable benefits to be attributed to the proliferation of strong and easily accessible cryptographic protocols. In order to estimate the value of encryption more precisely, new and better data will be necessary. First, we need industry-specific data that specifically addresses the amount of time, labor, and money that is invested in the maintenance, implementation, and use of encryption.

Second, we need a more specific estimate of the value the average online user places on secure communications—with a focus on the most common uses and applications of software-based encryption. These would include, among others, online banking, e-Commerce, and social media websites. Third, we need more robust data on the time individuals spend using services that utilize encryption. Fourth, we need more robust studies, using experimental economics or survey methods, examining the average user’s sensitivity to the level of security of websites and communications technologies. At the very least, these metrics can serve as more robust proxies for assessing the value individuals and firms place on encryption.

The concluding chart is a telling representation of the growth of all these measurements, as well as general Internet usage, and helps put all these metrics into focus.<sup>44</sup> In every

---

<sup>44</sup> [Note]: This graph compares each year of data with the base observable year. For example, if the first observed data point is 1997, each year shows the growth of that variable from that original data point in 1997. If the original observable data point is 2000, each following year will compare the growth of that

case, although the growth of certain variables may have slowed at times, the clear trend is one of growth across all examined measurements. While not necessarily establishing a causal link between the value of encryption and the growth of these industries and metrics, this assessment is clearly suggestive of a mutually reinforcing growth trend.

In 1999, Lynn McNulty, then the Director of Government Affairs for RSA Data Security, penned a report assessing the economic benefits associated with relaxing export controls on cryptography. In her conclusion she correctly pointed out the wise policy disposition U.S. policymakers should take vis-à-vis encryption:

The United States should nurture rather than impede this market as secure electronic communications networks have become an integral component of the global economy. Because computers store and exchange an ever-increasing amount of corporate-sensitive and highly personal information, including medical and financial data, it is necessary to secure such information from unauthorized eavesdropping and malicious alteration. Communications applications, such as electronic mail, electronic funds transfers, and on-line purchasing, require secure means of encryption and authentication. Such features can only be provided if cryptographic know-how is widely available and unencumbered by government regulation and outdated export controls.<sup>45</sup>

The value of embracing such encryption policies was true in the 1990s, just as they are today. Policymakers would be wise to remain hands-off when it comes to attempting to regulate the use and deployment of encryption and other online security products. The explosive growth of the Internet and ICT security has been the result of the government's willingness to embrace a non-interventionist approach to the online realm. The modern digital economy will only continue on its exponential path of development if that attitude continues to guide government policy.

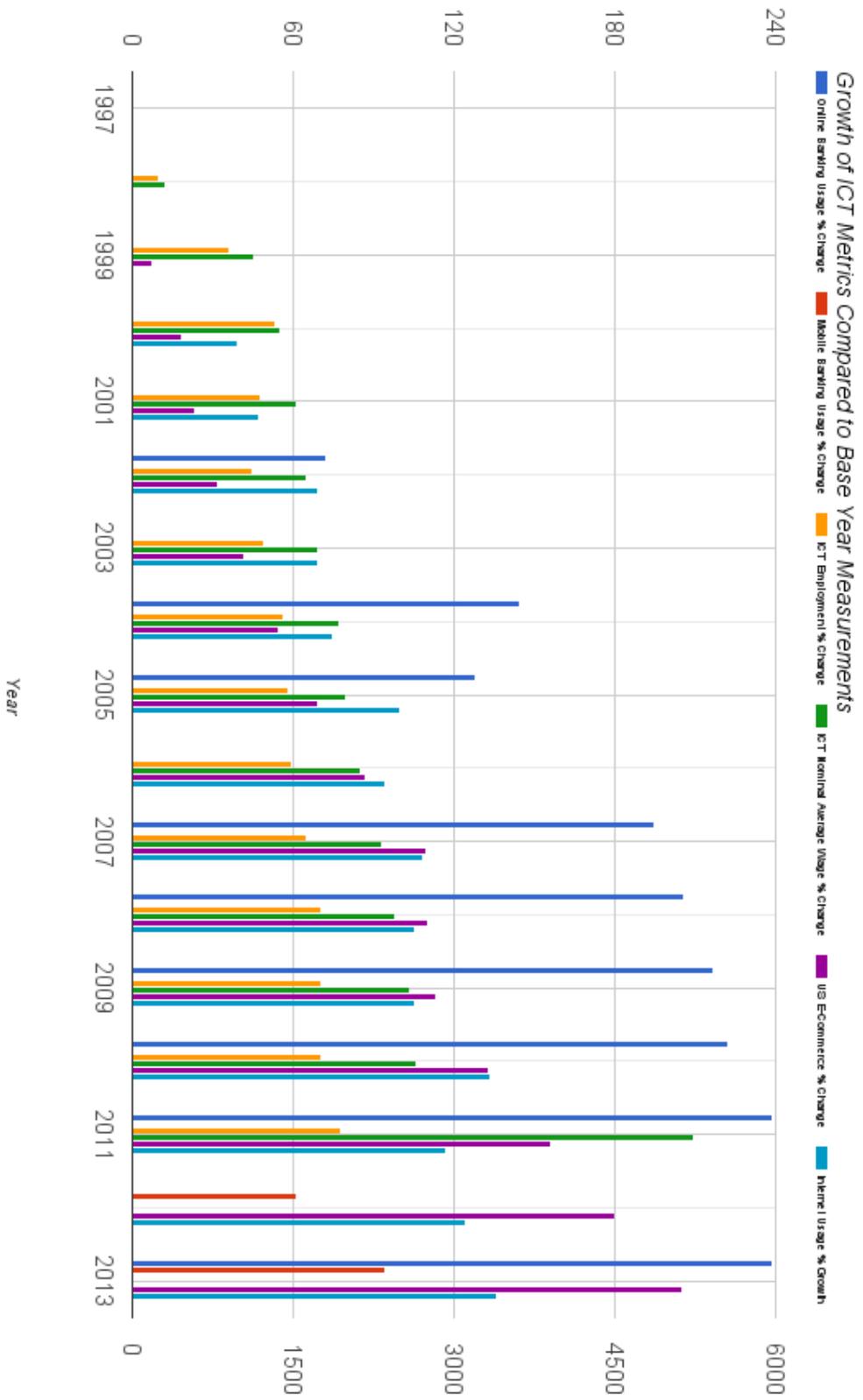
---

year with the original data point in 2000. This was done to show that although growth over time has slowed for most of the variables, the markets for each are substantially larger than when first measured. The base years for the variables are: Online Banking, 2000; Mobile Banking, 2011; ICT Employment, 1997; ICT Median Wage, 1997; US E-Commerce, 1998; US Internet Usage, 1997. It is important to note that e-Commerce is the only variable measured by the *right-hand axis*. This is because its growth relative to base was so massive it prevented the other variables from being viewable. For example, e-Commerce in 2013 was 5130.12% of what it was in 1998, its base year. All other variables are measured on the *left-hand axis*, where the highest measure is American Internet usage for online banking in 2013, which showed that the online population in the US was 238.89% higher than it was in 2000. The relative percentages were calculated by taken the observed year's data, dividing it by the relative base years, and controlling for the original amount. ((OY/BY) - 1).

<sup>45</sup> F. Lynn McNulty, "Encryption's Importance to Economic and Infrastructure Security," *9Duke Journal of Comparative & International Law* 427-450 (1999). <http://scholarship.law.duke.edu/djcil/vol9/iss2/4>.

The Internet is the lifeblood of the modern digital economy; encryption protocols are the white blood cells. The health of the Internet ecosystem depends on the proliferation of strong encryption.

All other % growth (relative to base)



E-Commerce % Growth (Relative to Base)