The Rising Importance Of Strong Encryption For U.S. Interests

By Christopher Hooton, Ph.D.

Internet Association

IA Report

Section A

Introduction

Encryption protects billions of global Internet users from countless daily threats to sensitive infrastructure, the financial system, and repressive governments looking to stifle speech and democracy. From policymakers to academics and industry leaders, the consensus is clear: strong encryption is fundamental to protecting our national interests.

The foundation of this consensus lies in the strategic utility, economic value, and technical realities of encryption as a proactive defense tool. Additionally, as this paper describes, the exponential growth of the internet is driving an increase in the risk factors associated with failing to enact strong encryption protections. These risks are not static. As the internet continues to expand into more corners of the American economy, our exposure to economic costs and security vulnerabilities grows along with it.

More than $1 trillion of U.S. economic growth is driven by the internet sector, representing six percent of total GDP (Internet Association, 2015). At a time when networks are nearing full integration, encryption is critical to shielding our citizens and companies from fraud, hacking, and corporate espionage by safeguarding everything from financial transactions to everyday consumer devices. Foreign and domestic threats have long gained notoriety for targeting private data in hacks aimed at internet companies and websites, representing an obvious threat to our nation's economic security.

But what's to stop hackers from draining value from the other 94 percent of the economy? Newly digitized systems incorporated into hospitals and banks represent incredible opportunities for efficiency and growth, but they also create vulnerabilities. If exploited, these integrated systems could cost billions of dollars and completely disrupt the American way of life.

Encryption is critical to shielding our citizens and companies from fraud, hacking, and corporate espionage by safeguarding everything from financial transactions to everyday consumer devices.

These are not just idle concerns. In March, 2016 the U.S. charged state-sponsored hackers for attacking key financial networks. However charges won't stop hackers from trying. In fact, the attacks are becoming more frequent and concerning – in that same month, Iranian government hackers attempted to compromise a dam in Rye, New York, and just this month it was reported that state-sponsored hackers were looking to break into accounts belonging to journalists. These all serve as potent reminders of the importance of properly securing our ever-expanding digital world.

Strong encryption is our best tool in the 21st century for ensuring that the damage and costs of cyberattacks, data breaches, and other types of exposure remain minimized. It is a cost-effective and powerful way to reduce

the economic incentives of many cyberattacks. Further, it minimizes the damages and helps protect the crucial interests of our country and its citizens. As put succinctly by the Congressional Encryption Working Group[1] in their December, 2016 working group report, "Any measure that weakens encryption works against the national interest."

Section B

Expert Consensus

To be clear, the internet industry has a strong appreciation and respect for the efforts of law enforcement and intelligence agencies to keep Americans safe. These efforts to protect Americans allow our economy to flourish and grow in the long-term. The internet industry categorically abhors criminal and terrorist incidents and constantly endeavors to make our products safer while supporting law enforcement through data requests in response to valid legal processes. It is precisely because of its support for law enforcement and intelligence agencies that the internet industry also supports strong encryption.

In some respects, we have been lucky up to now. We have experienced a rise in both the number of breaches and the total number of exposed data records over the past decade, particularly among malware, phishing, and hacking (Verizon Enterprise Solutions, 2016). Yet, we have also lived with relatively little exposure and still have time to recognize the looming rise in online security risks. This luck will not continue.

Given advances in computing, reduced costs, and increased skills of would-be attackers, data breaches are becoming more dangerous and harder to detect. Data and their production are forecasted to continue rising exponentially, and the trend of data record exposure (via breaches) will also move upwards, reflecting the sharp 48 percent increase in 2014 in detected cyberattacks of any kind (PricewaterhouseCoopers, 2015). The sophistication and frequency of attacks that lead to security breaches have grown dramatically due to increased connectivity and greater potential economic gains from attacks (Chris Fischer in Allianz, 2016). Indeed, these worries are paralleled by the relentless increase in concern among cybersecurity practitioners seen in the Index of Cybersecurity since its first observation (Healey, 2016; Geer and Pareek, 2016).

It is precisely because of its support for law enforcement and intelligence agencies that the internet industry also supports strong encryption.

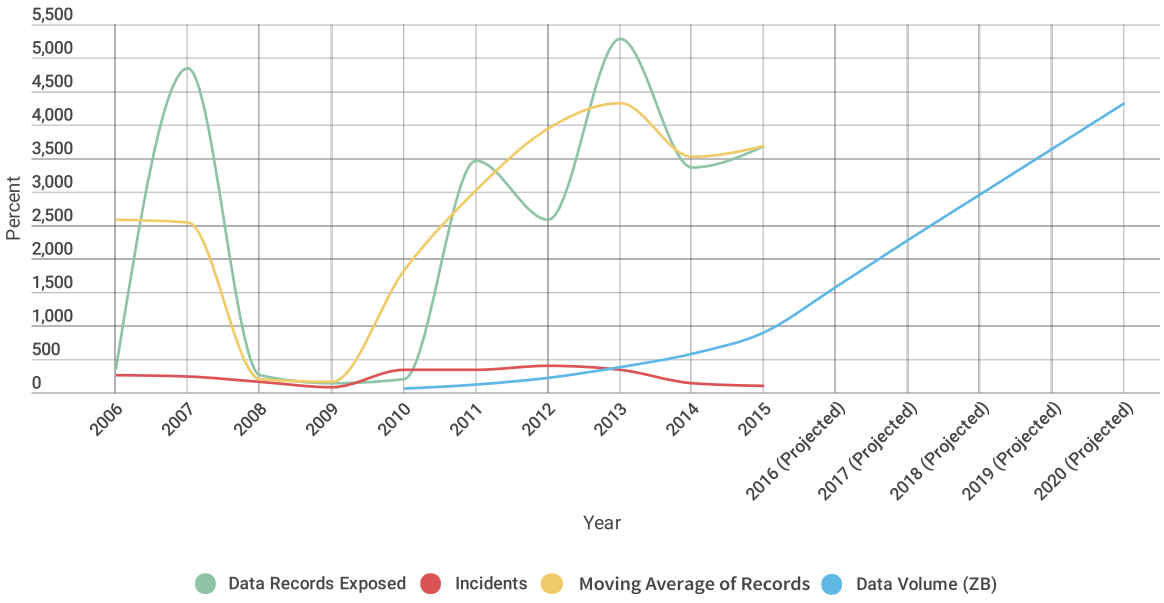
Security breaches are not limited to hackers or rogue organizations. State-sponsored cybercrime is increasingly a threat, especially from China. Its economy is a powerhouse and developing dynamically, but it does not

[1] *A joint working group comprising of members from the House Judiciary Committee and House Energy and Commerce Committee.*

yet rival the U.S. in technological development or innovation. Many Chinese industries have calculated that it is cheaper to copy American intellectual property (such as designs, software, and corporate strategy), than to develop their own products. These firms have turned to hacking as a replacement for research and development. As former national security officials Mike Mcconnell, Michael Chertoff And William Lynn (2012) have said, “the Chinese government has a national policy of economic espionage in cyberspace.”

CHART 1: PERCENT GROWTH SINCE 2005

The Real & Potential Damages Of Data Breaches Are Growing Total Data Production Volume



Source: Privacy Rights Clearinghouse (2016); (Computer Sciences Corporation, 2015); forecasts calculated by author

Section C

Understanding the Nature of the Risks

Beyond broad calls and technical details, it is important to understand how the nature of data breaches and security risks bolster the need for strong encryption. More specifically, it is crucial to understand the concentrated nature of breaches and the growth in exposure risk.

Using data on security breaches since 2005 from Privacy Rights Clearinghouse (2016), this paper’s analysis demonstrates that a majority of damage comes from large ‘outlier’ events – or those with record exposure volumes greater than 3 standard deviations from the average. While these events comprise only 0.5% of all security breach incidents, they contribute 80% of the total number of records exposed. This suggests that while the volume of incidents themselves are high, security efforts cannot be concerned with only providing shields that solely seek to manage incidents at

Security efforts must be concerned with the potential damages of every single incident and seek the broadest implementable defense technology across all users and technologies – encryption.

an 'acceptable' level.[2] Rather, security efforts must be concerned with the potential damages of every single incident and seek the broadest implementable defense technology across all users and technologies – encryption.

We can see this utilizing the simple cost impact model for data breaches from Jacobs (2014), which was also used by Edwards, Hofmeyr, and Forrest (2015) specifically with Privacy Rights Clearinghouse data, to illustrate the major potential financial costs that every single breach incident can have. The average annual costs of security breaches from 2005-2016[3] are estimated to be more than $5.5 billion with large outlier incidents comprising approximately $3.4 billion of that total.[4] On a per incident basis, large incidents have caused approximately $1.65 billion in damage per incident over the same period. Compare that to the total expenditure of Fortune 1000 companies on customer cybersecurity of $2.4 billion per year, or approximately $2.4 million per company per year (Dwoskin, 2014), and we quickly see the cost-effectiveness of stronger encryption.

TABLE 1: SECURITY BREACH CHARACTERISTICS, 2006-2015[5]

Total Records Exposed	*Average Record Exposure Per Year*	*Total Estimated Impact*	*Average Impact Per Year*	*Average Impact Per Incident*	*Average Impact Per Record*
1,796,389,628	149,699,136	$66,132,390,985	$5,511,032,582	$29,870,095	$36.81
Large Incident Outliers - Number of Records	*Large Incident - Average Record Exposure Per Year*	*Total Estimated Large Incident $ Impact*	*Average Large Incident $ Impact Per Year*	*Average Large Incident Impact Per Incident*	*Average Large Incident Impact Per Record*
1,436,327,993	11,969,400	$41,232,345,689	$3,436,028,807	$1,649,293,828	$28.71

Source: Data from Privacy Rights Clearinghouse (2016); impact estimates calculated utilizing impact model from Jacobs (2014)

It should again be emphasized that the risk and costs of security breaches are not static, but instead are set to increase dramatically. This increase in risk stems from exponential growth in data production and processing power that provide a greater motivation, and means, for would-be attackers. The greater integration of data into new systems leads to new risks for individuals (Orcutt, 2016). However, we have the opportunity now to encourage and implement strong encryption which can fundamentally shift the dynamic in favor of defense while also strongly diluting one of the major motivations for attacks. Encrypting data helps render data largely useless for those without security access and, subsequently decreases the value of that data

[2] *As a useful metaphor, vaccinations require a critical mass of a population to receive them, rather than every single individual, in order to be effective; however, such an approach would not work in cybersecurity because of the great damaging potential of every single incident.*

[3] *2016 contains partial observations for part of the year.*

[4] *Cost estimates are calculated using the model from Jacobs (2014).*

[5] *See Appendix for further details on nature of privacy breaches.*

In the view of Internet Association, the only effective way of providing both the necessary breadth of security and the intensity to secure against potential major individual events is through strong data encryption.

for resale. Put differently, encryption provides a two-pronged approach to cybersecurity: it severely reduces the likelihood of damage – financial and otherwise – from breaches and, it also reduces the motivation to seek or cause breaches at all.

Unencrypted data are now a threat to nearly every industry and nearly every internet user. Unfortunately, some data are left intentionally unprotected due to misguided popular or government pressure. The potential damage is growing tremendously and we must reframe how we consider the impacts of cyberattacks and data breaches. In the view of Internet Association, the only effective way of providing both the necessary breadth of security and the intensity to secure against potential major individual events is through strong data encryption. Encryption is at the epicenter of cybersecurity; it is the core component of protecting data.

Section D

A Brand New World

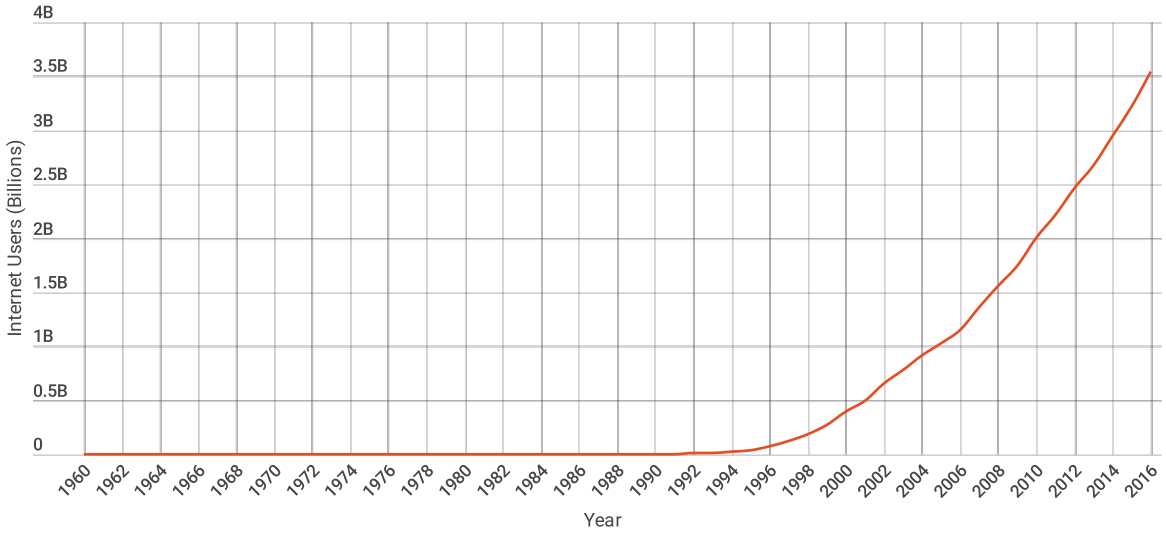
In the 21st century, we have moved into a new world with different resources, interests, and risks. It is dangerous not to recognize and protect them.

Arguably, this shift has been most prevalent and obvious in the development of computers, information technology, and the internet. While these areas developed over many decades, it is only in the past 15 years that we have seen massive growth in their reach and capacity.

In particular, there are three important metrics from an encryption risk standpoint. The first is the number of users of the internet, which has grown from approximately 2.6 million worldwide in 1990 to over 3.2 billion in 2015, according to The World Bank (2015), and an estimated 3.5 billion in 2016. Second, total data volume production will increase to approximately 35 zettabytes in the year 2020, an increase of more than 20 times the 2009 level (Computer Sciences Corporation, 2015). And third, computer performance – as measured by computing power index developed by Nordhaus (2007; data from 2010 online Appendix)[6] – has grown by 264 times what it was in 2000. The rise of these three metrics over time are shown in Figures 1-3 and Figure 4 compares them standard growth metrics of population and GDP per capita.

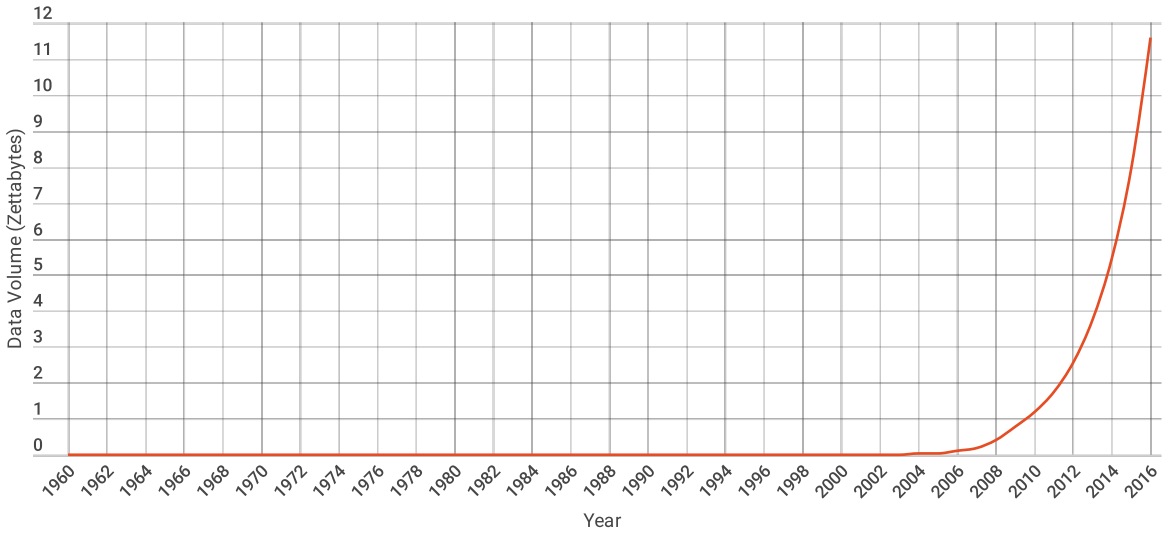
[6] *Future years estimated using standard AR(2) time series approach. As a robustness check, the paper compared these with alternative computational metric developed by Hooton (2016) based on hardware capacity metrics.*

CHART 2: GLOBAL INTERNET USERS



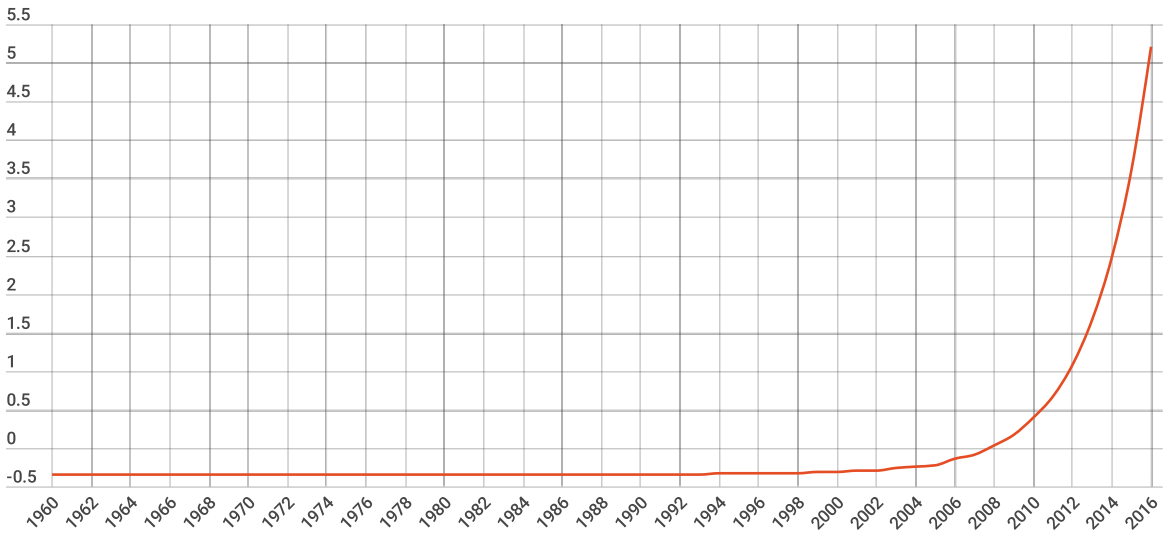
Source: The World Bank (2016)

CHART 3: DATA VOLUME (ZETTABYTES)



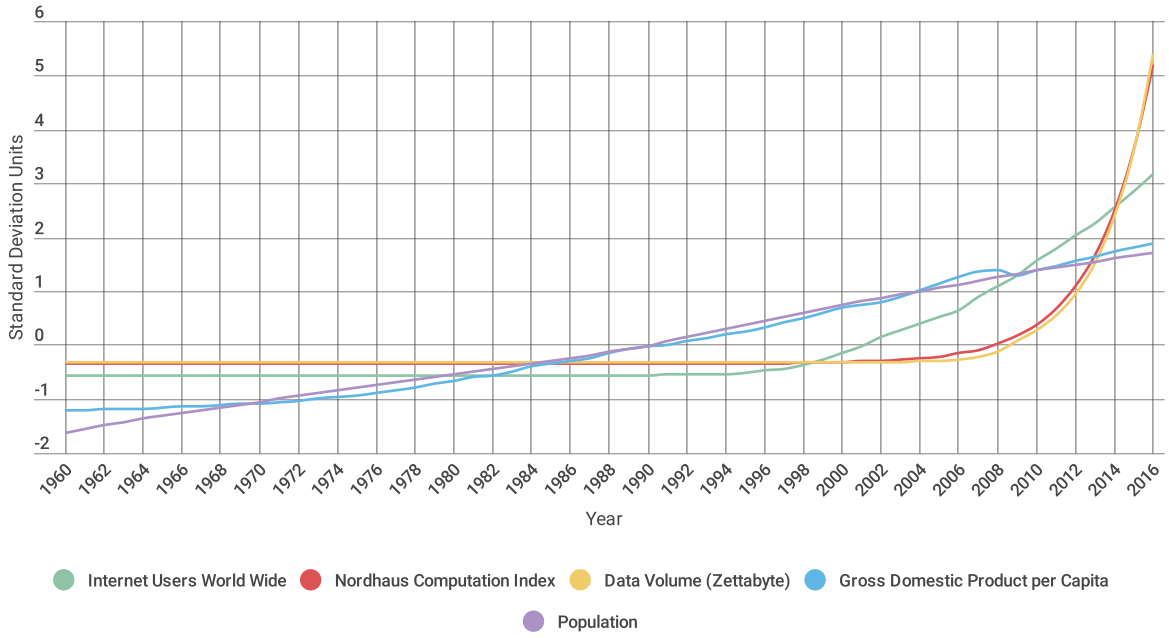
Computer Sciences Corporation, 2015

CHART 4: NORDHAUS COMPUTATIONAL INDEX



Source: Nordhaus (2010); forecasts calculated by author using autoregressive model

CHART 5: INTERNET COMPONENT GROWTH VS. TRADITIONAL GROWTH METRICS



Source: Nordhaus (2010); Computer Sciences Corporation (2015); GDP and Population figures from World Bank (2016)

Why are these metrics important? They demonstrate a dramatic increase in risk from cyberattacks, data breaches, and other incidents relative to the growth of our economy. The sheer number of internet users increases the potential targets for cyberattacks while the growth in data production volume increases the number of potential records that can be exposed. There are more people using global internet systems and there is more information available

The sheer number of internet users increases the potential targets for cyberattacks while the growth in data production volume increases the number of potential records that can be exposed.

for attackers to use. Additionally, the costs of computing and the rise of computational power have now universalized the ability to conduct such attacks. Anecdotally, we can recognize this power in the smartphones we carry in our pockets, but on a more sophisticated level there are no longer significant 'barriers to entry' for would-be attackers. Malicious intent and capacity have been democratized, and the damage could be immense if we do not catch up on the protection front.

As a thought exercise, if we assume that the potential costs of breaches are a function of total data production and then forecast record exposures based on forecasted data production (Privacy Rights Clearinghouse, 2016), we see the dramatic rise in risk. Table 2 illustrates that, in the absence of better defenses and a continued increase of exposures, the potential costs could easily jump into the hundreds of billions each year.

TABLE 2: ESTIMATED POTENTIAL RISKS 2016-2020

	Average Records Exposed Per Year	*Average Impact Per Year*
2006-2015	149,699,136	$5,511,032,582

	Estimated Records Exposed Per Year	*Estimated Impact Per Year*
2016	1,820,455,189	$67,018,341,791
2017	2,847,504,958	$104,828,210,898
2018	3,874,554,726	$142,638,080,005
2019	4,901,604,495	$180,447,949,112
2020	5,928,654,263	$218,257,818,219

**Note: Estimations assume exposures are direct function of data production volume; calculated using data production growth rates weighted by annual production average during observed period of 2006-2015.*

In the past, experts have noted how cybersecurity has protected hundreds of millions of people (Encryption Working Group, 2016), but in the future it will protect billions of people and this is precisely why strong data encryption is so important. No other tool can serve as a substitute for protecting national interests and minimizing the economic and social costs of breaches.

Section E

Conclusion

Every day we see the increasing importance of integrating encryption into our world. Security breaches and the volume of data exposed are increasing. As the risks and damages of exposure increase, so too do the consequences of failing to implement and support strong encryption. The internet industry understands the critical challenges facing law enforcement in this arena, which

We have grown overly dependent, economically and otherwise, on the benefits of secure communication and we cannot put American interests at risk through weakened encryption standards.

is precisely why it calls for strong encryption. This issue can be put simply: we have grown overly dependent, economically and otherwise, on the benefits of secure communication and we cannot put American interests at risk through weakened encryption standards.

If we are serious about national security in the 21st Century, we must have strong encryption as a core component in our defense. There are too many risks – from human error to state-sponsored hackers – and they are multiplying too quickly for us to ignore them. The costs of security breaches have been proven to be massive, both from a financial perspective and from the danger they present to increasingly integrated critical systems, such as power plants and schools. Strong encryption is critical to countering these growing risks; we must recognize that encryption itself offers the most powerful shield in protecting our economic and our national security.

Section F

References

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner. (2015). "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications." Computer Science and Artificial Intelligence Laboratory Technical Report. MIT-CSAIL-TR-2015-026. Massachusetts Institute of Technology.

Allianz. (2016). "A Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity." Allianz.

Computer Sciences Corporation. (2015). "Big Data Universe Beginning to Explode." Infographic. Accessed November 2016. Available at: http://www.csc.com/insights/flxwd/78931-big_data_universe_beginning_to_explode.

Dwoskin, Elizabeth. (2014). "Companies Are Spending More on Customer Privacy but It's Uneven: Survey." Wall Street Journal. November 6, 2014. Accessed December 2016. Available at: http://blogs.wsj.com/digits/2014/11/06/company-spending-on-customer-privacy-rising-but-uneven-survey-says/.

Edwards, Benjamin, Steven Hofmeyr, and Stephanie Forest. "Hype and Heavy Tails: A Closer Look at Data Breaches." Working Paper. Accessed December 2016. Available at: http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_edwards.pdf.

Encryption Working Group. (2016). "Encryption Working Group Year-End Report." House Judiciary Committee and House Energy and Commerce Committee. United States Congress.

Geer, Dan and Mukul Pareek (co-publishers). (2016). "Index of Cyber Security". Accessed January 2017. Available At: http://www.cybersecurityindex.org/.

Healey, Jason. (2016). "Defense at Hyperscale: Technologies and Policies for a Defensible Cyberspace." White Paper for Black Hat 2016. Columbia University School of International and Public Affairs.

Hooton, Christopher. (2016). "Exploring machine learning's contributions to economics productivity." Working paper.

Internet Association. (2015). "Measuring the U.S. Internet Sector." Internet Association. Prepared by Stephen Siwek at Economists Incorporated.

Jacobs, Jay. (2014). "Analyzing Ponemon Cost of Data Breach." Blog post. Data Driven Security. Accessed December 2016. Available at: http://datadrivensecurity.info/blog/posts/2014/Dec/ponemon/.

McConnel, Mike, Michael Chertoff, and William Lynn. (2012). "China's Cyber Thievery Is National Policy—And Must Be Challenged." New York Times. January 27, 2012. Accessed January 2017. Available at: https://www.wsj.com/articles/SB10001424052970203718504577178832338032176?cb=logged0.33303006598725915

Nordhaus, William D. (2007). "Two Centuries of Productivity Growth in Computing." The Journal of Economic History. Vol. 67, No. 1. (March 2007).

Nordhaus, William D. (2010). "Two Centuries of Productivity Growth in Computing." Online Appendix. Accessed December 2016. Available at: http://www.econ.yale.edu/~nordhaus/homepage/recent_stuff.htm.

Orcutt, Mike. (2016). "Security Experts Warn Congress That the Internet of Things Could Kill People." MIT Technology Review. December 5, 2016.

Privacy Rights Clearinghouse. (2016). "Data Breaches." Dataset. Accessed November 2016. Available at: https://www.privacyrights.org/data-breaches.

PricewaterhouseCoopers, CIO, and CSO. (2015). "The Global State of Information Security® Survey 2015, a worldwide survey by CIO, CSO and PwC."

Romanosky, Sasha. (2016). "Examining the costs and causes of cyber incidents." Journal of Cybersecurity. 1-15.

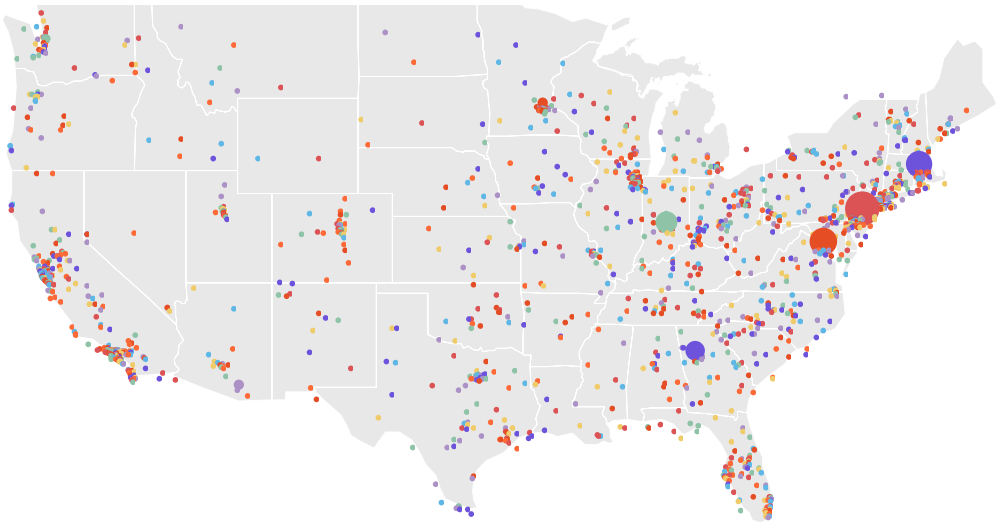
Verizon Enterprise Solutions. (2016). Data Breach Investigations Report. Verizon. Accessed January 2017. Available at: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

World Bank. (2016). "Internet users (per 100 people)." Dataset. The World Bank. Accessed December 2016. Available at: http://data.worldbank.org/indicator/IT.NET.USER.P2.

Section G

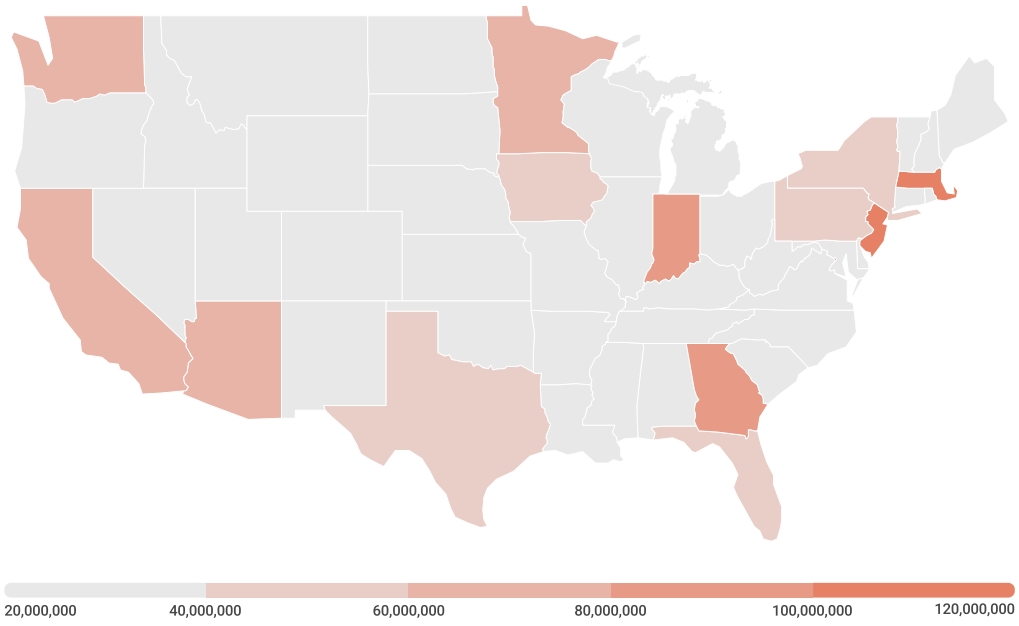
Appendix

MAP A1: DATA BREACHES BY PLACE



Source: Author's elaboration; data from Privacy Rights Clearinghouse. (2016).

MAP A2: DATA BREACHES BY STATE



Source: Privacy Rights Clearinghouse (2016); (Computer Sciences Corporation, 2015); forecasts calculated by author

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.