the digital equilibrium project

Advancing the Dialogue on Privacy and Security in the Connected World

March 2016

Copies of this report are available at the Equilibrium Project online: http://www.digitalequilibriumproject.com

Contributors

Stewart Baker

Former 1st Assistant Secretary of DHS
and General Counsel of the NSA
Partner, Steptoe and Johnson

Tim Belcher

Former CTO, RSA

Jim Bidzos

Chairman and CEO, Verisign

Art Coviello

Former Executive Chairman, RSA

Dr. Ann Cavoukian, Ph.D.

Executive Director of the Privacy and Big
Data Institute at Ryerson University

Larry Clinton

President and CEO
Internet Security Alliance

Michael Chertoff

Executive Chairman of The Chertoff Group
U.S. Secretary of Homeland Security '05-'09

Richard Clarke

Former White House Advisor
Chairman and CEO, Good Harbor Security
Risk Management

Edward Davis

Former Boston Police Commissioner
President and CEO, Edward Davis, LLC

Brian Fitzgerald

Chief Marketing Officer, Veracode

Kasha Gauthier

Program Committee Co-Chair, NICE and
Special Advisor, Boston College
Cybersecurity Masters Program

J. Trevor Hughes

President and CEO, International
Association of Privacy Professionals

Michael McConnell

Former Director of the NSA and
Director of National Intelligence

Nuala O'Connor

President and CEO
Center for Democracy & Technology

JR Williamson

Corporate Chief Information Officer
Northrop Grumman

Knowledge Partner:
McKinsey & Company

Foreword

"The release of atomic power has changed everything except our way of thinking... the solution to this problem lies in the heart of mankind."

Albert Einstein

Would you feel more secure knowing your government could listen to conversations between terrorists? Are you comfortable with the idea that your smart TV can listen to conversations in your living room? Are you glad that your increasingly intelligent car can save your life? Are you aware that it can be tricked into causing a fatal accident? Are you relieved your doctor can use advanced algorithms to help diagnose your illnesses? Are you concerned that corporations can use advanced algorithms to deny you healthcare? Do you know the insulin pump in your body can be adjusted without painful surgery? Do you know it can be wirelessly disabled without your knowledge?

The physics of the digital world are different from anything we've ever experienced. They ignore national borders. They smash together cultures, ages, continents, kids, adults, criminals, spies, geniuses and twenty-somethings into one global mosh pit, where laws, morals and politics fuse in ways we never could have imagined a few years ago.

Some of these possibilities and risks sound legitimate. Some might sound ridiculous. All are proven realities of the world we inhabit.

The physics of the digital world are different from anything we've ever experienced. They ignore national borders. They smash together cultures, ages, continents, kids, adults, criminals, spies, and geniuses into one global mosh pit, where laws, morals and politics fuse in ways we never could have imagined a few years ago.

We are unprepared for it. But we are charging ahead anyway, because humans explore, innovate, and execute. It is what we do.

We are unready because, at its heart, the internet is not just a technology. It is a new dimension where individuals, organizations and governments must interact in ways that are productive, safe and socially acceptable. But the laws, policies and social norms we have developed over centuries in our physical world are not capable of providing the structure we need to inhabit this new dimension peaceably, happily, and prosperously. The power we are unleashing with the internet and digital technology is very much like what Einstein alluded to with atomic power – it has already changed everything, except the way of thinking we will need to cope with it.

We see the results daily. Crimes unpunished. Loss of trust in governments and corporations. Undeterred foreign sovereign-directed attacks, without effective response. We are all digital citizens, but our digital society is a global, increasingly homogenous, and nearly lawless one that becomes more pervasive and important to us with each keystroke.

This is only the beginning. As another billion people join the global community, we are building upwards of 100 billion devices to join it: intelligent devices with embedded applications that will run our power grids, our hearts, our automobiles, our thermostats, our kids' new playthings. Without norms of behavior and standards for privacy and security, we will not know how to tell these devices to behave in this interconnected digital world, any more than we know how to tell ourselves or our children.

That may not sound like a big deal today, but the digital and physical worlds – "bits and atoms," as a recent article in the Economist referred to them – are increasingly fusing into one world where actions in one dimension have real implications in the other, with less knowledge of who is doing what to whom.

Our amazing technologies may be planting the seeds of disaster, even as they make tremendous improvements in our quality of life today.

Our amazing technologies may be planting the seeds of disaster, even as they make tremendous improvements in our quality of life. To avert disaster, we will need to rely not on new technology but on reimagining social disasters as old as human culture itself – breaches of the privacy and security that are essential to the smooth functioning of the physical world and perhaps even more crucial in the digital world. They are essential because trust in our privacy and security is the oil that takes the friction out of human interaction in all its forms. Trusting the sanctity of our personal information, our privacy, and our safety gives us the ability to barter, collaborate, and cohabitate as people and nations.

Reimagining privacy and security for the digital world is the essential precursor to building the laws, policies and structures that will avert the disasters described at the start of this note. Our project sets the stage for that essential work. It convenes disparate views on issues of privacy, government/citizen relationships, corporate responsibility and the relationships of nations in the digital world. It is about ending stalemate and fostering real dialogue that can help forge the laws, policies, and social norms needed to ensure we can all explore and harness the fruits of a peaceful, safe, and secure digital age.

We hope you will join the conversation.

Preface

In the earliest days of the Internet, privacy and security were at peace, mostly because they largely did not exist or even matter. The first internet was designed to share information between researchers. The concept of private communications was not a requirement. Before criminals, nations and hacktivists prowled the web, secure transfer of digital information was not necessary.

In fact, three men I know well, Ron Rivest, Adi Shamir and Len Adleman, arguably have had as much to do with creating today's expectations around privacy and security in the digital world as anyone. Building on the work of Whit Diffie and Martin Hellman, the question they posed in the mid-1970s was simple: "Could a message be sent on the internet that could be read only by the sender and intended recipient, without a prior relationship between the two?" They proved that in fact it was possible. The result was the RSA algorithm and the foundation for RSA the company (which I had the privilege to lead for many years). However, the implications of their work extend far beyond the borders of a single corporation.

A high level of trust in the privacy of our online communications became foundational to the explosion of the world wide web and our near-total reliance and faith in digital technologies today.

By standardizing, productizing and evangelizing their invention, the company they formed laid the foundation for authenticating and encrypting information on the internet at just the right time. Just as the internet became the world wide web, when browsers and commerce servers appeared in 1994 from Netscape, Microsoft and others, they were enabled with encryption technology from RSA.

This technology enabled the safe exchange of personal and payment information that is the underpinning of any commercial and consumer relationship.

They also put in motion the conflicting forces that today compete for control of the digital world. First, their work, and the tools built upon it, created an unprecedented expectation of privacy in online communications that became foundational to the explosion of the world wide web and our near-total reliance on digital technologies today. That implicit (and perhaps naive) faith fed our willingness to entrust the digital world with all manner of information about ourselves and our behaviors – information valuable to those who deliver goods and services we desire, but also to criminals, nation-states and others who wish to steal or repurpose that information. Second, by creating the concept of secure communications, they put the emerging digital world in the crosshairs of the world's law enforcement and intelligence agencies, who saw the explosion of digital communication and commensurate data-gathering capability as a gold mine for tracking the threats to citizens and nations. Those organizations saw their ability to listen to the digital world as an imperative – and that completely private communication was therefore anathema.

The result of that gap today is a growing tension between privacy and security – not only in our digital world, but also in the physical world that has become intimately and inextricably bound to it.

Today we stand at that crossroads: the pace of change and adoption of digital technologies continues to accelerate. From 2011 to 2015, the share of U.S. adults owning a smartphone nearly doubled, from 35% to 68%.[1] From 2010 through 2015, average daily internet consumption similarly doubled world wide.[2] This blinding pace of digital adoption has far outrun the laws, social norms and diplomatic constructs that we painstakingly developed over centuries to conduct affairs in our physical world. The result of that gap today is a growing tension between privacy and security – not only in our digital world, but also in the physical world that has become intimately and inextricably bound to it.

This is indeed the defining problem of the digital age. Whether we solve it will determine whether we are its masters or victims. It is what catalyzed our group, drives our work, and causes us to ask for your involvement. This work is essential to the continued economic, social, and political progress of our digital and physical world. It must begin now.

Art Coviello

1 Pew. Technology Device Ownership. Available online: http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/ Last accessed January 14, 2016.

2 Jason Karaian. Quartz. “We now spend more than eight hours a day consuming media.” Citing Optimedia survey. http://qz.com/416416/we-now-spend-more-than-eight-hours-a-day-consuming-media/

Privacy & Security in the Digital Age: The Case for a New Approach

What Are We Trying to Accomplish?

The goal of the project is not to provide a complete solution for the future of privacy and security in the digital world. Attempting to do so in isolation would be naive at best. Instead, our goal is to help define the problem in ways that embrace the many legitimate viewpoints of government, industry, and privacy advocates, and create forums for discussion where solutions to these problems can be advanced. An essential precursor to this dialogue is for all sides to move past oft-repeated misinformation that has crystallized into myth. Ultimately, our aspiration is to help stakeholders see privacy and security as two sides of the same coin, rather than zero-sum opposing views. After all, the only people benefiting from the status quo are the biggest threats to the privacy and security of all of us: criminals, hacktivists and the leaders of rogue nations.

Why Us?

The contributors to this project have a wide range of backgrounds and experiences. We are former senior members of America's intelligence and law enforcement communities, leading privacy advocates, technologists, cyber security professionals, lawyers, and business executives. A common passion unites us: changing the discussion around privacy and security in the digital age to foster real progress before it is too late.

The only ones benefiting from today's status quo are those who are the biggest threats to the privacy and security of all of us: criminals, hacktivists and rogue nations.

Despite our professional diversity, all of us save one are U.S. citizens. This is not because we believe this is a U.S. problem only – or that it can be solved entirely within the borders of any one nation. We start with the U.S. because it is the world's largest digital glass house. The massive social, economic, and infrastructure exposure of the U.S. to the digital world gives our nation both the most to gain from its safety and order, and the most to lose if order devolves. By starting where the problem is most acute, the stakes highest, we believe we can spark a discussion that will become global in scope.

Why Now?

For several years, privacy advocates have waged a two-front battle. First, they contest what they see as overly intrusive – even illegal – efforts by the U.S. and other governments to gain information about citizens and non-citizens in pursuit of national security. Second, they fight corporations who they believe are collecting massive amounts of information on consumers, often without their informed consent. At the same time, the intelligence community has followed the migration of communication from phone and paper to digital technologies of all kinds, harnessing the technologies' collection and analytics power to gain new advantages in support of their missions. In the commercial sector, organizations of all stripes have poured hundreds of billions of dollars into technologies and services designed to secure their digital infrastructures, even as outsiders comprised of state and non-state actors have extracted billions of dollars in value from unprotected or poorly protected corporate digital infrastructure.

Despite massive efforts on all these fronts, most Americans feel they are less safe and enjoy less privacy than just a few years ago. For example, fewer than 10% of Americans polled in 2015 were "very confident" that either the government, landline telephone companies, or credit card companies would ensure both the privacy and security of their records.[3] And the continued theft of intellectual property, financial data and personal information from organizations of all sizes is echoed by the concerns of information security practitioners who feel the task of defending their enterprises from all manner of digital attackers is harder than ever. For example, the number of records breaches reported in the U.S. grew at 29% annually from 2008 through 2013.[4]

Even as we slide backward in our pursuit of both security and privacy, the light-speed evolution of technology nears an inflection point that makes today's problems pale by comparison to what may come. By 2020, according to many estimates, we will see over 100 billion intelligent devices in use, all connected to our digital networks and systems. These devices will be capable of collecting data on nearly every aspect of our lives, including how we behave in our homes, how our children play, where we drive, how we manage our health and diet, and even how we live in our own backyards. The total economic impact of the internet of things could range between $3.9 and $11.1 trillion by 2025.[5]

Despite massive efforts on both security and privacy, most Americans would argue they feel less safe and enjoy less privacy than just a few years ago.

This explosion of devices will create an exponential challenge both for privacy (nearly every device in our lives will be a source of data for some provider) and security (the attack opportunities created by these devices will be literally a hundred times the level of risk we see in our digital infrastructures today). Unless we agree on principles to guide our social norms, laws, policies and diplomacy to address these changes, we can expect catastrophic outcomes in economic, social and even physical domains. These challenges are already with us. If we do not create constructs for addressing them today, we risk losing forever the ability to contain them.

Why You?

If you are reading this paper, presumably you have some interest in and perspective on security and privacy in the digital age. Our goal is to engage you in a constructive, open dialogue that can lead to real progress. It will take many perspectives – and significant commitment – to make real progress on these issues. Your engagement is what will matter most. Regardless of your perspective on the topic, we encourage you to keep an open mind. Challenge our thinking; consider how you could help advance the topic and shape the debate. We cannot use today's disagreements and experiences as reasons to withdraw to our separate corners while the hope and promise of our digital world are increasingly besieged.

But before we – and you – delve into those questions and their implications, we will explain how we have gotten here, the challenges of accelerating technological advances, and the implications for individuals, businesses, and world order.

3 Mary Madden and Lee Rainie. Pew Research Center. "Americans ' Attitudes about privacy , security and surveillance." 2015. Available online: http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ Last accessed January 14, 2016.

4 US-CERT.

5 McKinsey Global Institute. "Unlocking the Potential of the Internet of Things." June 2015. Available online: http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world Last accessed January 14, 2016.

Section 1. Setting the Stage

How We Got Here

It is a truism at best, and cliché at worst, to talk about the 'pace of change' in technology. However, as much as we comment on the continued advances and evolutions of technology, we still underestimate just how much it has evolved and how fundamentally it is shaping every element of our lives.

In the past decade, processing power has increased by greater than 20 times[6] while its cost has fallen to a small fraction of what it was.[7] With billions of transistors on a single chip, the internet of things is now possible and affordable. Internet traffic has increased by greater than 30 times,[8] making our devices chattier and digital communication something we take for granted. Storage capacities have increased by greater than ten times,[9] making collection – and retention – of information nearly free. Smartphone battery capacity has doubled, making mobility possible for increasingly powerful devices.

The pace of technological improvement outstrips the ability of even our most creative minds to fully predict or comprehend.

Each of these improvements by itself is comprehensible. Taken together, the systemic change is remarkable and unpredictable. For example, processing power, networking, geo-location, and software algorithms working together enable the self-driving car, the crowd-source navigation app Waze, and the behavior of the millions of drivers and passengers in the "crowd" who provide information for Waze in real time to make the service available. Massive increases in power and affordability on multiple dimensions simultaneously, leveraged by millions of entrepreneurs world wide, fueled by tens of billions of dollars of investment, will continue to unleash capabilities we can't anticipate even a few years before they become real, and shortly thereafter, ubiquitous.

The pace of technological improvement outstrips the ability of even our most creative minds to fully predict or comprehend. In addition, it totally overwhelms the ability of our social systems to keep pace. Our social norms develop slowly, through consensus and shared experience. While the industrial revolution has been centuries in the making, for example, we are only recently coming to grips with its environmental implications and how to manage them. Today, the very definitions of what it means to be human are being called into question by advances in genetics and artificial intelligence. Is it any wonder that our definitions of privacy, for example, based on our experiences in the physical world over hundreds of years, are no match for the scenarios emerging daily in the lightning-fast evolution of technology?

6 Growth in number of transistors per commercially available microprocessors for 2005-2015, using the Pentium D Smithfield from 2005 (~169M transistors) and the Intel 18-core Xeon Haswell-BP (~5.IB transistors). Wikipedia. MIT Review.

7 http://www.singularity.com/charts/page62.html

8 Cisco. 1.3 exabytes/month from 2004 to 42 exabytes/month in 2014. Available online: http://blogs.cisco.com/sp/the-history-and-future-of-internet-traffic. Last accessed January 14, 2016

9 Extrapolated from International Data Corporation showing data storage capacity growth of ~9x from 2006 to 2012. Wikipedia. Available online: http://wikibon.org/wiki/v/Announcement Brief: IBM SONAS Enterprise NAS. Last accessed January 14, 2016.

The same factors hold true on the individual front. Consumers are worried that corporations are eroding privacy and that their personal information can be stolen in cyber-attacks on organizations they trust, while the disclosures of Edward Snowden and others stoke additional fear, uncertainty and doubt. The result is a society worried, frustrated and unsure how to respond. Ironically, many people direct those frustrations at the very enterprises and governments trying to serve them, losing sight of the fact that the cyber-attacks on those organizations have arguably the most direct impacts on the sanctity of their personal information and financial and physical security.

The result is a society worried and frustrated, but unsure how or where to direct those frustrations. Ironically, they often direct those frustrations at the very enterprises and governments trying to serve them.

Similar factors play out in the relationships between nations. The interconnectedness of the digital world has blurred the definition of national sovereignty even as it creates new vectors for espionage, theft of intellectual property, and even destruction of property and infrastructure. Classic definitions, rules, and agreements fail in this new environment. For example, why is a digital incursion into a corporation that sits on American soil not treated the same way as a physical incursion would be? As we move towards the internet of things, the ability of one nation (or non-state actors in one nation) to cause physical harm to citizens in a different nation is growing rapidly. Without agreed-upon mechanisms to address grievances created by those actions, nations act alone to support their interests . At current course and speed, we should expect catastrophic digital conflicts between nations, with physical consequences. Perhaps even more frightening, non-state actors, terrorist groups, and even individuals will find it easier to acquire and use these destructive capabilities.

By nearly every measure, we are losing on both sides. Those who fight for privacy see it eroding at every turn; those who are dedicated to securing our nation, our corporations and our citizens from digital attacks are finding their task harder and more thankless than ever.

At current course and speed, we are moving towards an era where we should expect catastrophic digital conflicts between nations with physical consequences to occur.

Our path – fast, rocky and contentious – is not sustainable because technology is about to enable a step-function increase in the ubiquity of digital infrastructure and how deeply it pervades our lives. That step function is the internet of things.

Crossing the Chasm; the Fusion of the Digital and Physical Worlds

As noted, as many as 100 billion intelligent devices will be connected to our digital networks by 2020. These devices will occupy increasingly intimate and crucial roles in how we drive our cars, secure and manage our homes, educate our children, grow our food, deliver energy to our cities, and conduct nearly every other aspect of our lives.

These devices are doing more than adding massive scale to our digital infrastructures. Their very nature adds new urgency and new complexity to the security/privacy debate. Why? Because they represent a tipping point where our physical and digital worlds become irrevocably fused, as do our risks and social issues.

Why such dramatic consequences? Three reasons:

1. **The increasingly critical role of these devices in our lives, coupled with limited abilities to manage and secure these devices, will add entire new categories of risk, both digital and physical. This will not go unnoticed by nation-states and non-state actors alike who will explore both the defensive and offensive implications and opportunities created by the extraordinary increase in attack surface.**
2. **The intimate role of these devices in our lives, coupled with their ability to collect and share all manner of information about their (and our) status and behavior, will render some of our most basic constructs of privacy obsolete.**
3. **The ability of these devices to lower costs and create value for corporations, while adding convenience and new services for consumers, will make their rapid proliferation inevitable, even as angst over both the security and privacy of our world becomes more acute.**

While the U.S. may be the world's largest digital glass house, we can expect a global "digital housing boom." Economies world wide will be increasingly based on digital foundations, resulting in increasing sensitivity to the risks and opportunities for their wealth and safety that are already seen in more digitally advanced economies. For example, the number of countries with 4G mobile network access has more than quadrupled to more than 80 since 2011. Each of these nations adds global citizens to the mix along with new perspectives on privacy and trust in the interconnected global dialogue.

As the social and legal underpinnings of our integrated physical and digital world become increasingly unstable and ineffective, the costs potentially are incalculable.

The Implications:

The path outlined above threatens to turn our nation-level digital glass houses into a global house of cards. This increasingly powerful and essential digital infrastructure will sit on an ever-less-capable or relevant set of social, legal and diplomatic constructs that are unable to ensure the security and privacy of individuals, organizations and nations.

Our nation-level digital glass houses could become a global house of cards. Our increasingly powerful and essential digital infrastructure will sit on an social, legal and diplomatic constructs that are ever less able to ensure the security and privacy of individuals, organizations and nations.

As the social and legal underpinnings of our integrated physical and digital world become increasingly unstable and ineffective, the costs potentially are incalculable. Let us repeat that: incalculable. Since economic trade depends on trust, we can expect increased friction in global trade as trust between nations erodes. Intellectual property theft, for example, already costs the US more than $300 billion annually.[10]

10 The IP Commission Report, 2013. p.11
Available online: http://www.ipcommission.org/report/ip_commission_report_052213.pdf. Last accessed January 14, 2016.

If the return on investment in innovation falls due to piracy and theft, we can expect enterprises to either rethink their investment strategies or pressure their governments for increased intervention in forms that could foster embargoes, tariffs and other forms of trade war. As our digital devices "cross the chasm" and become intertwined with our physical world, the likelihood of physical harm becomes nearly certain. Digitally connected cars, trains, power grids, medical devices and so on create opportunities to reduce many of today's risks, but all represent opportunities for new forms of calamity. Already we see isolated examples sensationalized in the media. History shows that we can expect today's "proof of concept" hacks to turn into tomorrow's weapons.

History shows that we can expect today's "proof of concept" hacks to turn into tomorrow's weapons.

In summary, the friction and risk arising from a lack of new norms and constructs for digital privacy and security will fall into three categories:

- **Economic:** Increased friction in the global economy could cost at least $1-2 trillion annually in just a few years. The longer-term threat to trade and globalization and its economic consequences are indeed incalculable, but tens of trillions of dollars could be at stake.
- **Existential:** As digital exploits increasingly cause physical and economic harm, the risk of existential catastrophe becomes very real, either directly (exploiting flaws in digital security to disable power grids, for example), or as second-order effects (digital attacks or conflicts between nations escalate into traditional kinetic conflicts).
- **Societal:** Even if we avoid existential catastrophes, the loss of trust between consumers and providers or citizens and their governments, driven by continued erosions in privacy, will reduce our willingness to use digital technologies freely in communication, collaboration and innovation in every aspect of society.

Section 2. The Failure of Today's Debate, and the Opportunity for a New Approach:

A famous self-help book, "What Got You Here Won't Get You There," suggests that once you have achieved a certain level of career success, getting to the next level demands new skills and approaches.

Unfortunately, when it comes to privacy and security, we cannot even claim success to date. The polarization of the discussion, the vested self-interest of parties on all sides, and the challenges that come from creating lasting consensus in a rapidly changing world have conspired against practical discussion.

Getting to the next level will demand new skills and new approaches.

What we propose:

- A new approach that is balanced and sustainable, based on creating not detailed polices or legislation but a framework for creating those instruments – a constitution, if you will, not a book of laws. This framework must embody basic beliefs and guiding principles that will be meaningful beyond any evolutions of technology so that it can guide the evolution of our laws and policies as technology changes.

- A set of structures for continued dialogue and problem-solving, so that continued rapid changes in the landscape of society and technology can be understood and incorporated into policy, law and public discourse.

- A framework that builds on successes and finds and leverages analogies to today's world in free trade, diplomacy, law enforcement and social norms, while embracing the unique characteristics of speed, scale and change that are hallmarks of our new digital age.

Section 3.
A Structure for the New Approach

We hope this paper and the work that follows can lead to that framework. And we intend to start that action by inviting the many voices who need to be represented, those called out in this paper and others who wish to contribute, to come together in Washington for a mid-year meeting to begin the real work of building the solutions framework – the "constitution" for the digital world.

Our vision for that mid-year meeting is to begin developing recommendations that can evolve into a framework to be acted on by industry and presented to the incoming administration. Our belief is that these recommendations can be a springboard to a global conversation and ultimately a better and safer digital world.

To write this paper, our group collaborated in two day-long meetings, complemented by several months of research, interviews with stakeholders in business, privacy and government, and a myriad of individual discussions. We came to understand that the scope and complexity of the problem were part of the reason solutions and action have been so difficult to come by. Working together, we developed a structure built around four fundamental questions that address key dimensions of the problem. We offer that structure here as a way to inform future discussions.

We invite all the contributors to this debate to come together in Washington for a mid-year meeting to begin the real work of building out the solutions framework – the 'constitution' for the digital world.

We thought of the problem along four dimensions: to explore privacy and security relationships within organizations; between consumers and providers; citizens and their governments; and between nations themselves. We asked ourselves and others a fundamental question about each of these areas. Moreover, we gathered input and reactions that add depth and clarity to the questions themselves. Again, our intent was not to provide final answers but to put enough shape, substance and granularity to their dimensions to make real progress possible.

This section of this paper will be devoted to providing some depth and color to the following four questions:

1. What practices should organizations adopt to achieve their goals while protecting the privacy of their customers and other stakeholders (e.g., privacy by design)?

2. How can organizations continue to improve the protection of their digital infrastructures and adopt privacy management practices that protect their employees?

3. What privacy management practices should governments adopt to maintain civil liberties and expectations of privacy, while ensuring the safety and security of their citizens, organizations, and critical infrastructure?

4. What norms should countries adopt to protect their sovereignty while enabling global commerce and collaboration against criminal and terrorist threats?

We believe that cutting the Gordian knot of the privacy and security debate into these constituent parts can make progress during the next rounds of dialogue more productive. Eventually, these threads will need to be knit back together into a strong fabric that unifies the varied points of view and challenges represented in each, since each domain has implications for the other. For each question, we provide an examination of the question itself, a starting hypothesis for the issue, and a "blueprint for dialogue" to help drive future discussions towards action.

Question 1: What privacy management practices should organizations adopt to achieve their goals while protecting their customers?

When it comes to personal information and its potential uses by corporations and other organizations, many elements work against transparency.

On its face, this question would seem to be simple to resolve. In an open market, consumers could simply choose to do business with providers of goods and services who managed personal information in ways the consumers accept. Market forces would strike the natural balance between privacy and convenience, just as they do with prices, quality and other aspects of a free market.

However, those market forces can only work when there is transparency – when both sides know what they are trading and open communication can enable the market, over the course of many transactions to settle at its "natural" level. When it comes to personal information and its potential uses by corporations and other organizations, many elements work against that transparency:

The pace of change

Technology changes so fast that every element, from the ways information can be collected and what information is possible to collect to the ways it can be leveraged for profit or organizational gains, is in constant flux. Consumers can't anticipate all the ways information about them can be collected or used, and organizations can't perfectly predict all the ways they may wish or need to capture and use information in the future. And legislators can't write laws that target specific technology, collection techniques or uses of information that remain relevant for long, or for societies to avoid unintended consequences from legislation as the technology landscape continues to shift.

The growing value of insight and analytics

Even if organizations could predict their own needs, the competitive advantages of unlimited access and use of information are massive. Many organizations use customer information to deliver more value for their customers in the form of more targeted products, faster responses to changing needs, and more efficient delivery of goods and services. So organizations are inherently motivated to seek new ways to use that information, and are usually rewarded for their efforts by increased revenues or more satisfied customers.

The risk of 'privacy arbitrage'

The massive differences in national laws that regulate the collection and use of digital information can, over time, create significant imbalances in the abilities of organizations to compete against better-informed, faster-moving rivals. Commercial organizations in particular will be tempted to look globally for the lowest bar to privacy, and assume any higher bar will inhibit their ability to compete.

Despite those challenges, we believe that elements of an open market can improve the relationships between consumers and providers of goods and services. What follows here are the sorts of proposals we have discussed and believe illustrate the broader discussions that need to take place.

We believe that elements of an open market can improve the relationships between consumers and providers of goods and services.

STARTING HYPOTHESIS

- While perfect transparency is impossible, organizations could make significant progress by clarifying and simplifying privacy statements. Consumers who understood information collection practices could make informed choices, even automatically if privacy policies are machine-readable, and help establish a more market-based approach to establishing norms. So far, most machine-readable approaches have failed, but they should not be discarded as technology advances.

- Limits on the use of PII, such as one-time use of health information, may be embedded in policy, but it would be a major source of friction, preventing rapid advances in everything from healthcare to economic productivity. However, while all the future uses of information may be impossible to predict, privacy statements could embrace broad categories of use that consumers could choose to accept or deny, based on their willingness to contribute their information to the organization. Choice and notice themselves are not new, but more transparency will allow consumers to make more intelligent choices about the use of their personal information and ensure privacy by design.

- Some forms of a "transactional model" could allow for a more continuous negotiation of privacy agreements between consumers and providers. Moreover, we might change the balance of power: rather than force consumers to navigate complex legal language with every service, why can't they set the parameters and require the service providers to demonstrate they can honor them? Machine-readable parameters set by consumers, if made practical, could enable a more fluid transaction-based approach to negotiating privacy between these parties.

We submit that the focus on certain kinds of information-collection, mostly related to consumers, could hamper massive progress in areas such as health, medicine and education. Accidentally creating constraints on these well-meaning, well-governed practices to put short-lived (and probably ineffective) restraints on corporations in unrelated fields would be one of the biggest tragedies to date in our nascent digital history.

THE BLUEPRINT FOR DIALOGUE

Whom We Invite to Help

Building practical models for a more transaction-based, flexible approach to privacy between consumers and providers requires many voices: EPIC, the Center for Democracy and Technology, IAPP, the Electronic Frontier Foundation, the National Chamber of Commerce, the Business Roundtable, and others could play a role. The scientific and research community and the technology industry should join the discussion so the potential societal gains of information-collection and analytics can be weighed against the commercial benefits and consumer risks.

Open questions to help facilitate the dialogue:

- What is the commercial incentive for companies to be more transparent toward their customers and better stewards of their privacy?
- How can we make it easier for organizations in regulated sectors to wrestle with overlapping or conflicting regulations?
- What forcing function can drive enough momentum to overcome the inertia of incumbents that benefit from the status quo?
- How can we define data retention and usage guidelines? With what degree of granularity by industry? By use case?
- How can the concept of private and public space (with varying expectations of privacy) be related to the digital and cyberspace?
- Who else should be at the table, including representatives of different generations and those who can drive political impact?
- How can we ensure that commercial relationships evolve to match changing expectations?
- How can we reconcile the view of those who consider privacy an absolute right with those who consider it obsolete? And how can we satisfy those who fall between these ends of the spectrum?
- How can we design solutions flexible enough to account for changes in technological and behavioral norms?

Question 2: How can organizations continue to improve the protection of their digital infrastructures and adopt privacy management practices that protect their employees?

This question, like the prior one, would seem relatively simply to answer. Let's take the second part first. Employees work for their companies, and companies have a right and obligation to protect their assets and reputations, including gaining information about their employees.

Background checks for example, are an accepted part of the application process for many organizations today. As to the initial part of the question, the exploding capabilities of the digital world offer powerful new means for organizations to defend themselves, even as those capabilities have proven to give attackers new means of attaining their nefarious goals.

Board-level governance would need to mature quickly to provide context for technical investments and policy creation.

Unfortunately, neither question is so simple. Protecting digital networks today is not simply a function of building walls and barriers to hide behind (or to use the language of the Information security world, implementing firewalls and Intrusion Prevention Systems). As digital infrastructures become more fluid and software-based, organizations will be left with only two constants upon which they can focus: their users and the applications with which those users interact. While great scrutiny of users and quality of applications is a must, security also will require deeper insight into the behavior of systems and information, so the subtle, anomalous behaviors that are signs of compromise can be spotted and remediated. But in many nations, for example, worker privacy laws prevent collection of the very kinds of information that are essential to performing that monitoring task. As we continue to blend our professional and personal lives (and both become increasingly digital) pressure will continue to mount on employers to defend networks, but to do so without inadvertently trampling on the privacy rights of employees.

Those challenges cannot be addressed at a technical level alone. Boards of directors could play a far larger role in developing policies for privacy and security. They would need to understand digital risks as well as they understand financial and operational risks today, and be able to assess the competence of their information security programs. Most boards today are woefully unprepared on both accounts. Board-level governance would need to mature quickly to provide context for technical investments and policy creation, or security and privacy practitioners will be caught in the crossfire between employee demands and their respective job requirements.

The immaturity of corporate governance related to digital issues is not the only challenge, however. The following are even more acute:

- Organizations face a quagmire of contradictory or outdated laws and regulations; laws to protect worker privacy, for example, can make use of new behavior-based security technologies that help protect that privacy, actually illegal to implement.
- Personnel for both policy creation and security program management are hard to find. The current skills gap in information security alone is estimated at 300K-1M workers, and will only worsen as the landscape evolves. Without talented and trained professionals to help solve this problem, we will fall further and further behind.
- The complex nature of organizational supply chains, partnerships and business relationships makes the surface area of risk that must be defended nearly infinite in scope.

Even the largest and best-funded of security teams feel their defenses are immature and inadequate in the face of the risks they confront.

It's no wonder security teams often feel helpless or un-equipped to meet their challenges no matter how much they spend. While Gartner predicts global IT spending on security to top $100 billion by 2017, a study of IT and risk professionals by one large IT security company (RSA) shows that even the largest and best-funded of security teams feel their defenses are immature and inadequate in the face of the risks they confront.

STARTING HYPOTHESIS

- Business, academic and public sector partnerships could help create a larger flow of qualified cyber professions, both in the technical and policy/leadership domains.
- Boards of directors could add new members that offer the new skills they need, and can collaborate to create more shared knowledge and perspectives.
- Employees in privacy-oriented nations could recognize that they have more to lose by not empowering their security professionals than they do to gain by adopting inflexible postures on privacy: and enterprises could do a better job of providing transparency so their employees know how their information is being collected and protected in the workplace.
- The quality and security of applications, networks and identity management programs could be held to a level closer to that of automobiles, foods and other products where risk of flaw or compromise can lead to significant harm.
- Information sharing partnerships could continue to grow (see FS-ISAC as a model of progress in this area), built around mutual shared-interest such as supply chains, leveraging maturing models for sharing indicators of compromises and the evolving tools, tactics and procedures of adversaries.
- Integral and increased investment in new security capabilities as applications or services are developed will be required, and needs to be considered as essential to digital innovation as HVAC systems are to buildings.

THE BLUEPRINT FOR DIALOGUE

Whom We Invite to Help

Myriad organizations can play a significant role in advancing the answers to this particular question. They include the Internet Security Alliance, the National Association of Corporate Directors, the International Association of Privacy Professionals, the National Infrastructure Advisory Council, the Operation Resilient Shield exercise team, the Cloud Security Alliance, The Information Sharing and Advisory Councils, The National Initiative on Cyber Education, FIDO (Fast Identity Online Alliance) and various government agencies.

Open questions to help facilitate the dialogue:

- How could governments borrow from the nuclear (or other) industry to create and clarify a government role to help corporations protect their critical infrastructure from attack while managing privacy and security interests?
- How might corporations and corporate boards re-think their governance and oversight programs? (e.g., Center for Audit Quality, National Association of Corporate Directors)?
- How could we re-work the compliance v. cyber balance so that companies spend more time focused on value-add cyber security strategy and less on compliance-related work?
- How could we develop enough talent to keep pace with the evolving needs of all the related fields and industries?
- How could we create a forcing function or criteria for strong application, networks and identity management programs to ensure corporations are adequately protecting their employees and customers?

Question 3: What practices should governments adopt to maintain civil liberties and expectations of privacy, while ensuring safety and security of its citizens and critical infrastructure?

The underlying privacy relationship between citizens and their government is as old as societies themselves, and has often been uneasy.

This question has been at the heart of much of the public and media debate in recent years, spurred by the release of classified documents by Edward Snowden and accusations of impropriety against the NSA for collection and use of digital information. The underlying privacy relationship between citizens and their government is as old as societies themselves, and has often been uneasy. However, in the digital world the ability to collect and analyze massive amounts of information without transparency to the public, coupled with the increasing digital footprint of all citizens, takes the issue into new dimensions. And the issue will become more explosive through refinement of technologies such as facial recognition, which will enable identification of individuals any place where a camera exists (which today, is already ubiquitous).

In terms of our collective physical safety, this question is, in the short term at least, the most pressing to make progress on, but perhaps the most difficult as well. Terrorist organizations use the internet (and offshoots such as the so-called 'dark web') in a variety of ways, from recruitment and propaganda to planning and coordinating activities. Cybercrime costs the world's economies more than $445 billion annually.[11] But as individuals, corporations, nations, criminals and terrorists all increasingly roam the internet together, enabling governments to protect their citizens without compromising the privacy and trust of those citizens is increasingly difficult. Here is where the most dogmatic lines seem to be drawn between privacy advocates and security professionals (including military and law enforcement).

Cybercrime costs the world's economies more than $445 billion annually.

Interestingly, in this regard the challenges faced by enterprises and governments have many parallels. Just as organizations are adopting new approaches to information security in the face of eroding perimeters and increasing connectivity, government must find ways to defend their citizens in the face of porous national borders, increasing global flow of individuals and the democratization and ubiquity of communication made possible by the internet. Increasingly, that strategy will rely on even more information and better analytics, which, without proper governance, will further exacerbate the concerns of privacy advocates and citizens. The dearth of skill and expertise in the commercial world for cybersecurity will be a factor here as well, as governments seek to protect critical infrastructures from digital and physical attack.

11 Center for Strategic and International Studies. Net Losses: Estimating the Global Cost of Cybercrime. June 2014.

STARTING HYPOTHESIS

- Government could play a bigger role in helping define the 'how', not just the 'why' of protecting critical infrastructure, building on the NIST cybersecurity framework.
- Government could provide proper incentives for corporations to invest in cybersecurity for critical infrastructure.
- Governments could develop and enforce safety standards for software used in critical infrastructures.
- Governance and transparency could be strengthened for intelligence agencies, so that citizens can have confidence those agencies are working within the laws and guidelines that are in place.
- Government could communicate more clearly both the intentions and realities of intelligence gathering efforts. The Edward Snowden disclosures and ensuing outcry saw little to no clear, productive communications response by the White House or Congress. We need rational, fact-based debate and deliberation that result in clear action.
- Legal limits to domestic military involvement can be re-thought: digital tools can now create kinetic actions to cause real physical harm to our infrastructure (as was proven by the Stuxnet-based damage to Iranian nuclear centrifuges). The role of the military in defending US citizens could be re-defined to extend to cyber defense on U.S. soil, without running afoul of legal and constitutional constraints, or increasing the worry of citizens as to their privacy and basic freedoms.

THE BLUEPRINT FOR DIALOGUE

Whom We Invite to Help

Government needs to take the lead on this issue, but since critical infrastructure represents an intersection between the public and private sector, government must partner with the commercial sector and others such as EPIC, the Center for Democracy and Technology, IAPP, Electronic Frontier Foundation, the National Chamber of Commerce, the Business Roundtable, and others. The tech community must also move past simply disagreeing with government-led efforts, and begin recommending acceptable alternative solutions that leverage the skills and perspectives of our best innovators.

Open questions to help facilitate the dialogue:

- How should governments approach attribution and retribution to find and punish culprits of cybercrime in all its forms, even across national borders?
- When, if ever, should private companies be allowed to "hack back" and retrieve their stolen information before it's gone for good?

- What types of meta-data should be allowed to be collected and analyzed and what should the governance model be to ensure against actual or inadvertent abuse?
- How can we ensure transparency over law enforcement and defense activities without compromising their missions?
- How can spending resources be pooled between governments to, e.g., improve prosecution rates for cyber criminals (now at 2-3%)?
- Can/Must governments be more proactive, not just reactive/defensive post-attack?
- What does the hierarchy of threat, attack, and proportional government response look like?
- Should government be sharing more information?
- Is there a "NIST 2.0" to create, which is more actionable and easier to use?
- How can the cyber reinsurance market be leveraged or expanded to help?

Question 4: What norms should countries adopt to protect their sovereignty while enabling global commerce and collaboration against criminal and terrorist threats?

As long as there have been nations, there has been espionage. Spying on enemies (and friends alike) has been a known responsibility and set of actions by governments of all stripes.

Sometimes spying is (somewhat) benign, such as simply determining a nation's bargaining position on key issues; sometimes it is far more sinister in its intentions. Signals intercepts have been a part of those efforts since the days of the horse-mounted courier. In the digital world of course, espionage takes on a whole new complexion. Spying on communications has never been easier (for governments with the proper skills), and as more information of every form has become digital, more governments have gotten into the business of spying on behalf of their local corporations, in the form of intellectual property theft and communications intercepts.

When these actions become public, the outcry is understandably great. The action, however, is typically far more tepid. That is because the digital age makes the crimes of espionage at once more intimate and more difficult to prosecute. Intimate because the world largely shares one digital infrastructure, and a host of deep, complex trade relationships that makes commerce, communication and collaboration across national boundaries an absolute necessity. These crimes are more difficult to prosecute because the acts are committed remotely, through networks that make attribution difficult and evidence both ambiguous and highly technical. The perpetrators are (to the average citizen) nameless, faceless and abstract. So the outcry, while great, remains unfocused. And decisive actions by governments to address the concerns of their corporations and citizens becomes easy to avoid.

The U.S. may live in the largest digital glass house today, but a digital housing boom is under way globally.

STARTING HYPOTHESIS

We believe this situation will change. As the world becomes increasingly digital, the playing field will become more level. The U.S. may live in the largest digital glass house today, but a digital housing boom is under way globally. As more nations have more to lose by aggressive cyber activity against their allies and trading partners, pressure will mount to address this issue in a constructive way. Just as nations finally concluded that the long-term benefits of free trade outweighed the short-term benefits of capturing or sinking each other's ships on the high seas, nations will eventually come together to create digital rules of engagement. But why wait?

The risks in the meantime will remain high. Cyber intrusions that cause significant economic or physical damage create the possibility of escalation into traditional armed conflict. Even absent direct escalation into a shooting war, cyber attacks will increasingly cross the plane from bits to atoms and become kinetic in the damage they cause as we connect more of our devices to the internet. It is nearly inevitable that cyber attacks by nation states or terrorist will kill people at some point in time in the next few years. Keeping those incidents isolated, and containing their escalation into armed conflict is essential.

.

This is where nations must come together, to recognize the mutual interests in promoting clear rules of engagement and international law for the digital world. These agreements are not easy, but they are possible. We know nations are capable of reaching agreement on difficult and complex topics, as evidenced by the recent climate accords in Paris, where agreement was reached between 196 nations.

THE BLUEPRINT FOR DIALOGUE

Whom We Invite to Help

Governments must also take the lead here, but other organizations can play a role, including The Center for Strategic and International Studies, Carnegie Endowment, the Council on Foreign Relations, the International Institute for Strategic Studies, the Royal United Services Institute, Brookings, Yale Law, and the Global Commission on Internet Governance.

Open questions to help facilitate the dialogue:

- How could we limit cyber-espionage, to eliminate nation-states targeting individual corporations or organizations for economic or political motives? We believe that espionage will continue, but the current practices of many governments to use their national power to attack private institutions or other nations creates a dangerous imbalance and tips us towards broad-scale cyber conflicts.
- How could we collaborate globally, and empower existing or new institutions to track down international/domestic non-terrorist criminals?
- How could we create 'arms control' mechanisms to limit the spread of increasingly sophisticated malware tools? Unlike traditional weapons, cyber weapons spread rapidly, are quickly reproduced and modified, and are cheap.
- How could we address the issues of non-state actors who may target governments, enterprises or individuals across national borders? These actors often have multiple roles, working for their own goals as well as providing services to governments or other non-state actors.
- How could we create Mutual Legal Assistance Treaties? The US-China agreement to curtail economic-related cyber espionage, and even parts of model treaties offered by China and Russia at the UN could be useful starting points for what a nation state agreement could look like.
- How could we ensure that digital tools (software and systems) can be created free from nation-state interference (either overt or covert) so that these tools can be trusted by users globally?

Section 4. The Prize for Success and the Price of Failure

Today, cutting edge cancer research happens at the intersection of technology, biology, physics and mathematics. The impact of thousands of potential new drugs is modeled in computer simulations that would take years each to conduct using clinical trials. Massive data sets, not crowded hospitals are the source for knowledge – and the proving ground for advances that will perhaps save millions of lives in the years ahead.

Today, capital flows easily to where it can be put to best use, and investors have better insight than ever before into the most productive opportunities for their investments... increasing return for their shareholders but funding the innovations in every field that improve the human condition and create jobs around the globe.

Today we communicate, collaborate, buy, sell, trade and chat about everything in our lives using digital technologies that are already so ubiquitous we don't even notice them; but that are destined in short order to become exponentially more intimate parts of how we live- and how we can die.

Imagine for a moment if Rivest, Shamir and Adleman (and others like them) had come to a different conclusion: that trusted, private communication was NOT practical on the internet as we know it? What would our world be like today? The internet would in all likelihood have remained largely the province of academics and researchers. The world wide web (if established at all) would most likely become a tool for researching publicly-known information. But ecommerce as we know it would not be possible, and broad use of the internet by corporations would not be practical. The transformation we have witnessed over the past few years in how we work, live and play would be a slim fraction of what we now take for granted.

It is up to us to create the constructs that enable the digital age to mature into the force for good it has shown us it can be.

The digital age that's dawned for us promises the most rapid gains in wealth, health, culture and global collaboration we have ever witnessed. It is an adolescent at best, with physical attributes and energy that far outstrips its wisdom, experience and mature sense of right and wrong. It is up to us to create the constructs that enable the digital age to mature into the force for good it has shown us it can be. And to start on that path, it is up to us to form a new kind of dialogue, based on shared long-term interests and mutual trust between ideologies, economic interests and national agendas. Only by doing so can we create the same sort of constitution for the digital world that has served our nation so well in its history.

How to Get Involved

As we stated at the outset, progress on these important issues requires a multi-lateral discussion. Sustainable solutions must balance all perspectives against a set of shared goals and desired outcomes.

Copies of this paper are available at the following sites:

The Digital Equilibrium Project: *http://www.digitalequilibriumproject.com*

The International Association of Privacy Professionals: *https://iapp.org/resources/article/digital-equilibrium-project/*

The Center for Democracy & Technology: *https://cdt.org/insight/the-digital-equilibrium-project-balancing-privacy-and-security/*

The Internet Security Alliance: *http://www.isalliance.org/privacy/*

To inquire about participation in the mid-year conference, please email us at info@digitalequilibriumproject.com