The Data-Driven Economy as a Matter of National Security

Melissa Hathaway

26 October 2015

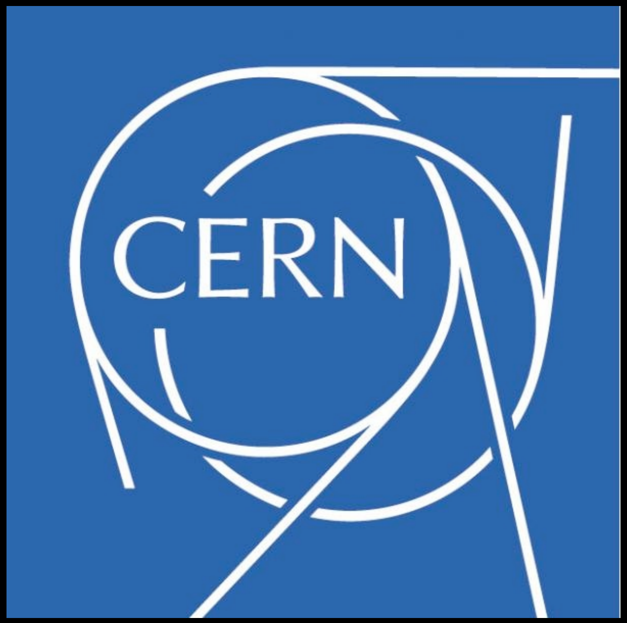
29 October 1969, the Internet Arrives!

Born from a Military Requirement

CERN Launched the World Wide Web, Enabling the Information Society and the Internet We Know Today

1990

Tim Berners-Lee



Switzerland

http://www.ncsa.uiuc.edu/SDG/Software/WinMosaic/HomePage.html

N C S A MOSAIC

NCSA Mosaic ™ for Microsoft Windows

Windows Home Page. Mosaic is a World Wide Web clien

on the campus of Th

1993

Constant Innovations - Change the Way We Live, Work, and Play

May 2000	GPS goes public — enabling proliferation of GPS-enabled consumer products
October 2000	AT&T introduces text messaging to the United States — instant text messaging for mobile phones
January 2001	Wikipedia came online, enabling a free user-generated online encyclopedia
January 2001	Apple launches iTunes changing the music and recording industry
March 2003	Social Networking launches with Friendster, inspiring others to follow - Facebook, MySpace, Twitter, LinkedIn, etc.
August 2004	Google goes public taking 65% of market share - embedding search as a way of life
February 2005	YouTube launched and revolutionized file sharing
November 2006	Nintendo launches the Wii and revolutionizes the video-games
June 2007	Apple launches the iPhone — smart phones advance mobile applications

The **Internet is the backbone** of family platforms, business engines, critical services and infrastructures, and the global economy.

Connecting Citizen Essential Services to the Internet Driving Efficiency, Productivity and the Economy

Industry & Manufacturing

Consumer

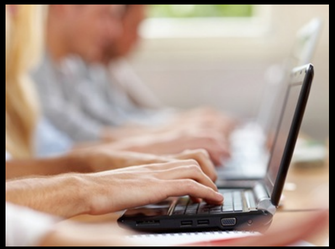
Buildings

Energy

Administration

Food

Space



ICT

Water

Chemical

Healthcare

Citizen Safety

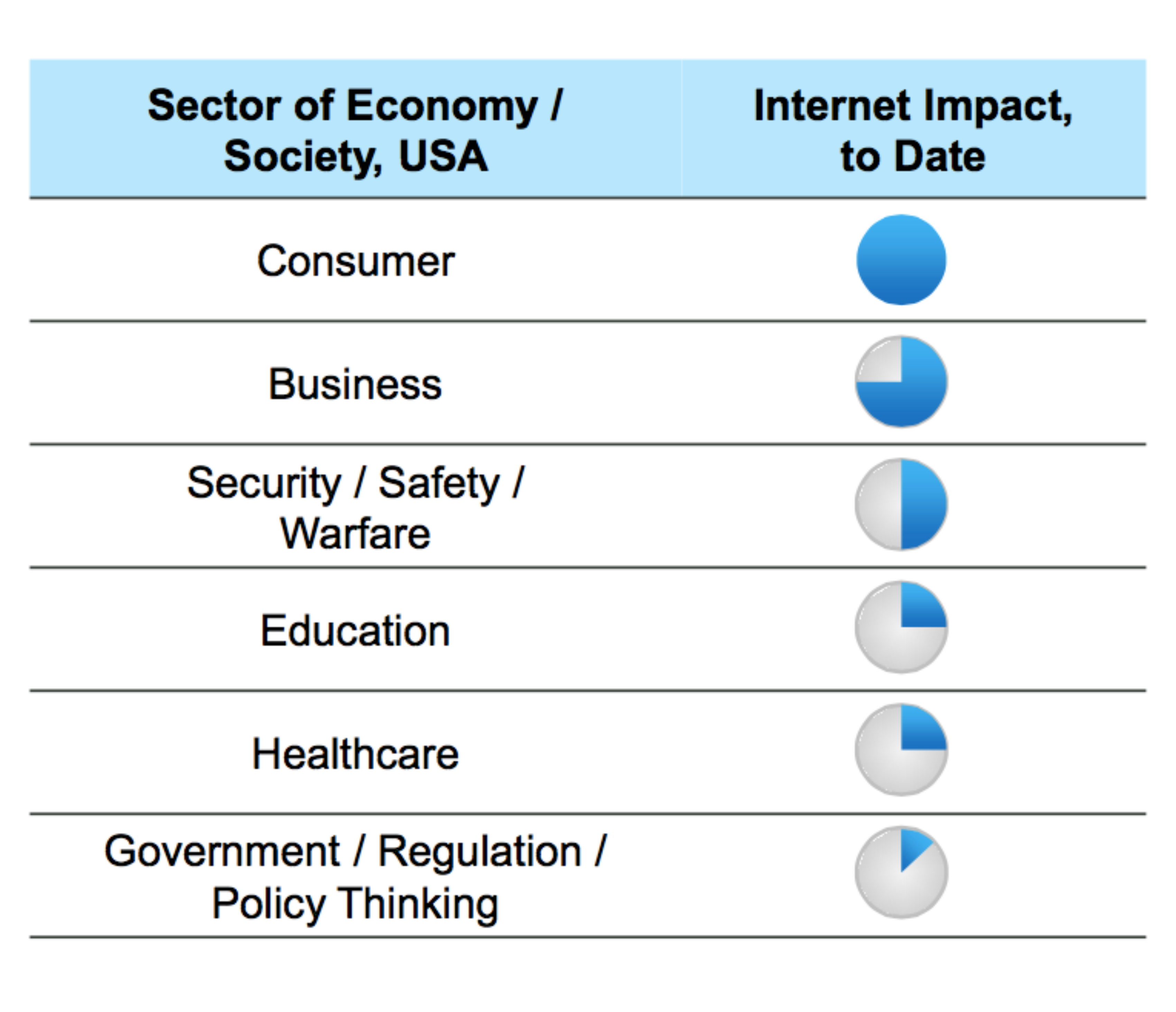
cash withdrawals
We won't charge you for cash withdrawals using your debit card
cash withdr

Financial Systems

Transport

Research

Our Digital Evolution is Just Beginning

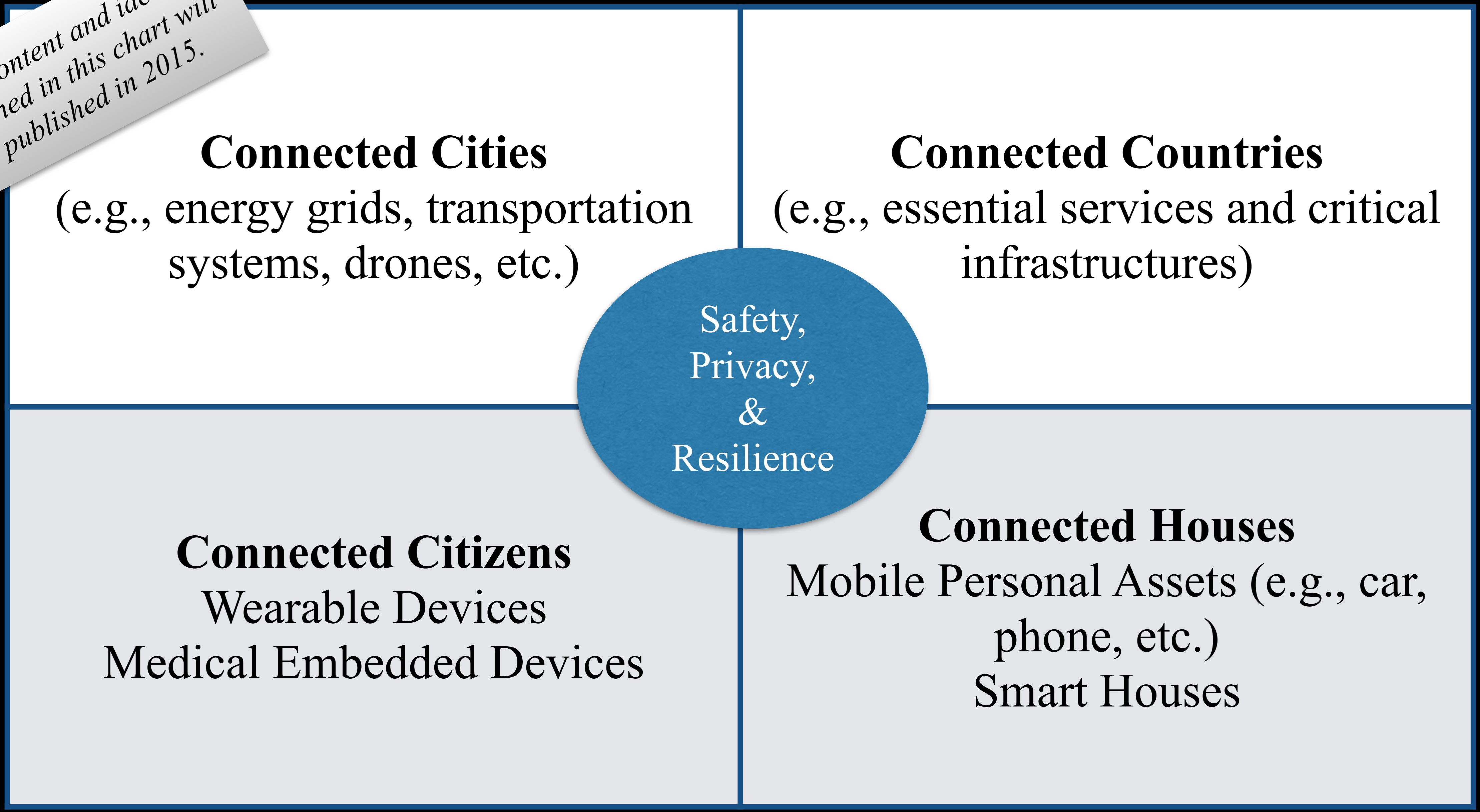


Sector of Economy / Society, USA	Internet Impact, to Date
Consumer	●
Business	◕
Security / Safety / Warfare	◑
Education	◔
Healthcare	◔
Government / Regulation / Policy Thinking	◔

Source: Meeker, Internet Trends 2015; KPCB.Com/InternetTrends

The Internet of Everything: Connecting Society in Unimaginable Ways

The content and ideas contained in this chart will be published in 2015.



Connected Cities
(e.g., energy grids, transportation systems, drones, etc.)

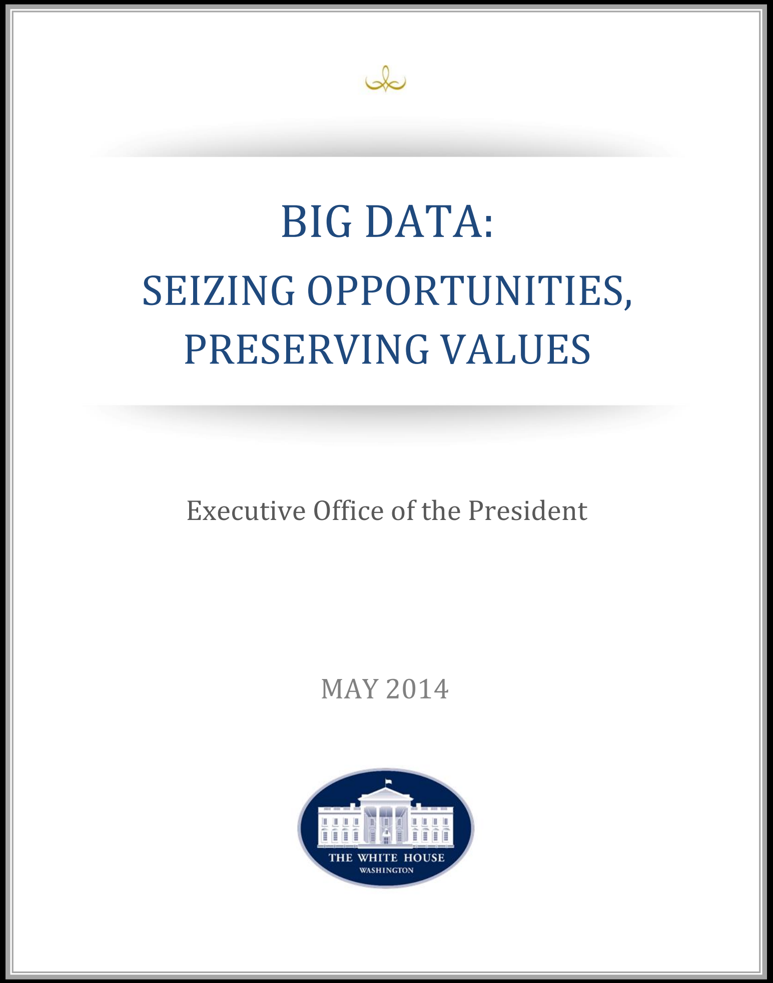
Connected Countries
(e.g., essential services and critical infrastructures)

Safety,
Privacy,
&
Resilience

Connected Citizens
Wearable Devices
Medical Embedded Devices

Connected Houses
Mobile Personal Assets (e.g., car, phone, etc.)
Smart Houses

Hyper-Connectivity Drives the Value of Data



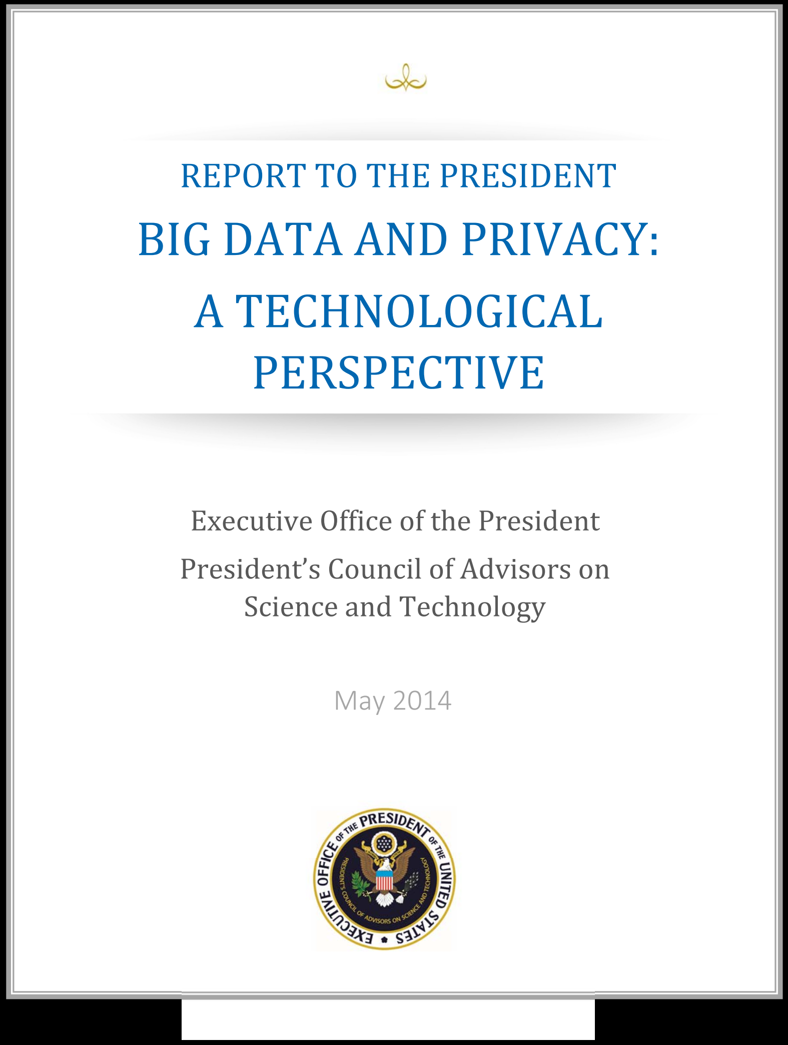
BIG DATA:

SEIZING OPPORTUNITIES,
PRESERVING VALUES

Executive Office of the President

MAY 2014

THE WHITE HOUSE
WASHINGTON



REPORT TO THE PRESIDENT

BIG DATA AND PRIVACY:
A TECHNOLOGICAL
PERSPECTIVE

Executive Office of the President

President's Council of Advisors on
Science and Technology

May 2014

The declining cost of collection, storage, and processing of data, combined with new sources of data like sensors, cameras, and geospatial technologies, mean that we live in a world of near-ubiquitous data collection.

The Digital Opportunity — Cannot be Ignored

$3.6 Trillion	2016 Worldwide ICT Spend
$19 Trillion	Near-Term Economic Opportunity: Devices that Connect People, Places and Things
$32 Trillion	Long Term Economic Opportunity: Modernizing Industrial Infrastructures (~46% of the Global Economy)
+4% to 10%	Anticipated GDP Growth: Connecting Citizens to the Internet

The economic opportunity of the Internet is at *risk*!

Activism, crime, fraud, espionage, disruption of service, and destructive activities are widespread.

The Internet enables a profitable underground economy — stealing our money, personal information, and intellectual property.

Anonymity and Asymmetric Advantage on the Silk Road…

- Advanced **targeted attacks** are bypassing traditional protection mechanisms and **persist undetected** in enterprises for extended periods of time (industry average is ~173 days).
  - The average cost per record in a data breach is approximately $275.00.
  - Most companies will spend over $1 million investigating and assessing a data breach.
- Interpol is mapping over 25,000 websites/spaces in the **DarkNet Information Market Place**, where you can buy personal identifiable information, military intelligence, weapons designs, and any other illegally copied data.
- Nations are no longer the sole customer for the “zero” day marketplace. **Anyone** with a credit card and access to the dark-inter-webs of the Internet **can purchase an exploit** and target your company or country.
  - Approximately 85 privately known exploits are available daily.
  - Most vulnerabilities remain undisclosed for an average of 151 days.
- Shodan software provides a **map of unprotected networked assets** including, power plants, medical devices, water treatment facilities, and traffic lights and is being used.

Policy and Law are Providing “Control” Points

- Target, December 2013
- United States - Office of Personnel Management, July 2014
- JPMorgan Chase Bank, October 2014
- Sony Pictures, November 2014
- Korea Hydro and Nuclear Power (KHNP), December 2014

The threat is outpacing our defenses, and

incidents will continue to increase in terms of frequency and gravity for the next three years

and

the costs will increase quicker than benefits.

Cyber *Insecurity* is a Tax on Growth!

GDP Erosion — Robbing our Future…

Losses	GDP Erosion	Cyber Activity	Country

€10 Billion	**~2%**	E-Crime;
		Identity Theft;
		IP Theft
			The Netherlands

$300 Billion	**~1%**	IP Theft	United States of America
€24 Billion	**~1.5%**	IP Theft	Germany
$4 Billion	**~.01%**	E-Crime	India

The Internet is becoming an instrument of control and suppression.

Policy and Law are Providing “Control” Points

- Australia passed a law (October 2015) **requiring** telecommunication companies to **store data for two years** — including data on who called or texted whom and for how long, as well as location, volume of data exchanged, device information and email IP data.
- France, UK, Canada, and soon to be the US have passed new **surveillance** laws - **deputizing Internet companies** (e.g., Facebook, Twitter, etc.) to report on suspicious activities to the government.
- Russia (February 2014), passed a **censorship** law demanding that ISPs **block access** to websites deemed to contain information promoting extremism and/or endangering public safety. The wording of this law can be broadly interpreted to “forbid pretty much anything critical of the ruling government: political opposition, environmental activism, provocative political art, investigative journalism, nonviolent political protest.”
- Prime Minister Erdogan instructed the ISPs operating in Turkey (March 2014) to **seal off access** to social media sites such as YouTube and Twitter to block citizens from organizing protests.
- Iran announced (2012) that it would pursue a **national intranet**, block services from Google, Yahoo, and Hotmail, and replace them with indigenous and government-led programs such as “Iran mail” and “Iran search engine” — in line with Iran’s plan for a “clean Internet.”

Policy and Law are Providing “Control” Points

- Russia passed a law (September 2015) requiring foreign organizations to conduct all primary **processing** of customer and client data **within** Russia’s **territorial borders**.
- German IT Law (July 2015) — ordering over 2,000 essential service providers implement new **minimum information security standards**.
- China published a draft cyber security law (July 2015) that broadly applies to the construction, operation, maintenance and usage of networks, as well as the supervision and management of cybersecurity within China. The draft law intends to **safeguard** China’s **cyber sovereignty**; protect against cyber-attacks; augment Internet security and safety; and regulate the use of personal data.
- The United States issued an Executive Order 13694 (April 2015) authorizing **targeted sanctions** against foreign individuals or entities whose actions in cyberspace result in significant threats to the national security, foreign policy, economic health or financial stability of the United States.

Policy and Law are Providing “Control” Points

- The Court of Justice of the European Union declared **Safe Harbor invalid**.
- The US DoJ vs. Microsoft - **compels access to customer data** (emails) maintained in a data centre operated by one of its subsidiaries located in Ireland — **undermining international law**.
- United Kingdom, India, Belgium, United States, and the United Arab Emirates — are considering legislation to compel companies to **hand over encryption keys** to aid law enforcement investigations and support national security matters.
- Others, including China, are demanding that companies that want to deliver products to their (broadly defined) national security marketplace must **turn over the source code** for their products.

The Internet is a swift delivery path for an arsenal of cyber-weapons.

Policy and Law are Providing “Control” Points

- Stuxnet;
- Rasgas;
- Saudi Aramco;
- South Korea’s Shinhan Bank;
- Sands Corp (Sands Casino in Las Vegas); and
- Sony Pictures.

SIEMENS

Stuxnet

신한은행
SHINHAN BANK

RasGas

ارامكو السعودية
Saudi Aramco

Sands
澳门金沙

Leaders are Trying to Set Rules of Engagement…

- The UN Group of Governmental Experts released a report (June 2015) outlining a common understandings of Information and Communications Technologies (ICT) and providing a framework for cyber norms — **setting standards for responsible state behavior.**

- Leaders from Brazil, Russia, India, China, and South Africa (BRICS) agreed that the potential **misuse of ICTs** for purposes which **threaten** international **peace and security** is of high concern.

- The OSCE adopted a first set of **Confidence Building Measures** (CBMs), aimed at **reducing the risks of conflict** stemming from the use of information and communication technologies (ICTs),

osce

Emphasis on the principles of international law enshrined in the UN Charter:
political independence, territorial integrity, and sovereign equality of states;
non-interference in internal affairs of other states;
and **respect for human rights and fundamental freedoms**.

The *end* of the Internet as we know it ?

Cyber-Insecurity — Challenging our Economic Future and Our Sense of Security and Privacy

- Fragmentation and regionalization of the Internet is underway;
- Western countries are abandoning the *OECD Principles* for a free, open and interoperable Internet;
- Democratic institutions cannot keep up - and the technology may challenge our values of democracy — Legislation and regulation are being used to limit Internet freedom;
- Increased use of surveillance - for "securing the state";
- Censorship is becoming more tailored;
- Regulated cooperation (e.g., Twitter, Facebook, Google assist law enforcement);
- Increased discussion on role of encryption and need for back doors;
- Distrust of Western standards; emergence of national standards and product testing facilities;
- Notion of privacy is challenged; and
- Protectionist policies emerging - data localization; product black-lists; and national champion preferences.

CTRL+ALT+DELETE:

It is Time to Reboot

Our

Cyber Future

Strong Leadership is Needed Now

1. Align the economic & national security agendas;
2. Engage in a national and international conversation regarding the IoT/IoE — architect for resilience, graceful degradation, and isolation;
3. Focus on three critical services/infrastructures — energy, telecommunications, and finance;
4. Clean-up infected infrastructures
5. Requires passion, persistence, partnerships, and political capital.

Cyber security is a necessary investment for the e-economy and our digital future

For other ***solutions***, please see:

http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html

❖

Melissa Hathaway

The Data-Driven Economy as a Matter of National Security

Melissa Hathaway

HathawayGlobalStrategies@Verizon.Net