Regulation of Digital Government

Michael Silverman

1 Introduction

National governments have established broad strategic statements of digital and technological aspirations. The advent of new technologies, ranging from cloud computing, the Internet, mobile devices, social media to on-line collaborative tools, have enormous potential to transform traditional processes of governance. But these new technologies come with significant, complex and daunting issues such as privacy and security, censorship, ownership claims, and health and safety concerns. The global nature of these technologies transcends national boundaries and permits the transmission of information to a global audience in seconds. This technology poses significant oversight challenges for governments' national sovereignty that traditionally control the means and access of information within their borders. Similarly, for the private organizations that supply and maintain the infrastructure of digital government, the growing requirements pose significant new regulatory duties and obligations. This Chapter examines some of the key issues that governments will likely encounter as they embark upon their transition to digital governments as well recommendations to address these concerns.

2 Regulatory Oversight

A folksinger once said that you do not need a weatherman to know where the wind is blowing. Similarly, the emergent digital government movement is inevitably faced with a number of regulatory challenges and requirements that govern its

M. Silverman (✉)
School of International and Public Affairs, Columbia University, New York, NY, USA
e-mail: ms2735@columbia.edu

S. Falk et al. (eds.), *Digital Government*, DOI 10.1007/978-3-319-38795-6_4

operations. Regulation is a powerful tool to control what government deems as risk. It can be used to control and influence data, determine access to information, decide which information is to be made public or held in secret, and where information is to be housed. It also plays a valuable role in enhancing transparency, predictability and the protection of citizens.

For modern organizations, whether in the public, private or non-profit sectors of the economy, the maze of regulatory demands imposes a significant requirement to ensure compliance with the letter and spirit of these obligations. Regulatory actions are in a constant state of movement. For modern organizations, it is often a constant struggle to understand and manage within this maelstrom of rules and regulations. The global emergence of the digital technologies has fostered an enormous growth of international, regional, and national regulatory oversight requirements. A former Chairman of a global European-based telecommunications corporation ruefully referred to this "universe of regulation" that his organization had to constantly struggle to manage within (Silverman 2008). Similar to its stellar counterparts, regulation is also forever evolving in form and fashion.

As governments move toward a digital future, they face a dual regulatory burden. While they are mandated to promulgate rules, regulations and guidance for non-governmental organizations, they are not exempt from the need to address the issues of regulatory duties within its own operations. The advent of the new digital technologies pose a particular challenge for governments who wrestle with the problems of governing Internet usage, social media, cloud computing, privacy and security concerns within their own operations.

2.1 Regulatory Tools

Modern regulation is a complex structure involving governmental and non-governmental players. The traditional concept of government "top down" rulemaking as the sole means for initiating and enforcing regulation must be seen in a changed context. Government regulations are now integrated with a variety of non-governmental regulatory bodies, e.g. professional groups (e.g. auditors, lawyers), standards–setting organizations and industry associations. Government regulations that encompass a range of mandates and obligations are often delegated to private organizations. These self-regulatory organizations (SROs) design rules and regulations governing their members' practices including setting standards, disciplinary practices, licensing requirements, and certifications.

This regulatory approach plays a key role in the administration of digital technologies and the Internet. Organizations[1] such the Information Systems Audit

[1]The diverse and fragmented governance of the internet include a number of other technical organizations responsible for coordination of the Internet infrastructure. In addition to the those named above there are IEFT (The Internet Engineering Task Force) which is a component of the

and Control Association (ISACA) and its COBIT framework for IT governance, or the International Organization for Standardization (ISO) and International Electrotechnical Committee (IEC) have issued numerous global standards for information technologies and to protect information assets. Probably the best-known non-governmental organization is the Internet Corporation for Assigned Names and Numbers (ICANN) who is responsible for registering Website domain names and IP addresses.[2] ICANN will be discussed later in this chapter.

3 Regulatory Challenges for Digital Government

The collection, storage and dissemination of electronic information associated with digital government is daunting. The trans-national character of most new technologies presents unique regulatory challenges. As governments increasingly focus on becoming, in the words of a government report, "information-centric, mobile enabled and collaborative digital environments," (Executive Office of the President of the United States 2012). The need to address these issues becomes even more challenging as the speed of new technological developments often outpaces the ability to regulate these technologies. One commentator wryly noted this challenge: "Trying to regulate the Internet . . . would be like trying to manage a transportation system in which not only new roads but new types of roads, and new types of vehicles, and new types of fuel, are invented each day. And the roads move, and hide. And some roads connect Alabama to Estonia, and are filled with invisible bandits" (Scholl 2012). Moreover, each of these technologies present their own particular challenges to government control and oversight.

3.1 Internet

In this era of Wi-Fi, broadband, email, cloud computing, social media, texting, mobile devices that are intrinsically part of so many of our daily lives, it is astounding to note that it was only in 1991, the first friendly interface to the Internet was developed at the University of Minnesota. The transformation has been staggering. In 2013, 44 % (3.1 billion people) of the global population was connected to the web (ITU 2014).

Never before has the wealth of information been so readily available. Digital technologies have transformed our lives—from access to medical information to

ISOC (Internet Society), IAB (Internet Architecture Board) RIRs (Regional Internet Registries), and W3C (World Wide Web Consortium).

[2]As of 2015 there are 156 countries, ranging from the United Arab Republic to Zambia who participate in ICANN's Country Code Names Supporting Organization (ccNSO).

personal relationships. Information on private and public sector performance, activities, and entanglements can be found sitting at a desk or on a train in almost any part of the world. Data that used to require hours, days or weeks to retrieve can now be found within minutes and then shared with others around the world shortly thereafter. The diverse access to this information is a staggering challenge for government regulators. No longer is access to Internet data limited to desktop computers with wired Internet connections. Laptops, smartphones, tablets permit Internet access often via wireless modems and fixed wireless Internet networks.

For governments wishing to pursue a digital future, the Internet, and its multiple means of access, are the backbone for new services and communications capabilities. While the Internet opened a new world of information and social communication, it also brought with it a plethora of major issues that will be discussed below: access to private information, fears of unauthorized intrusions, controversies over ownership and control of Internet content, and threats to national sovereignty and struggles with the best method to govern this new technology.

4 Social Media

The advent of social media, e.g. Twitter, Facebook, LinkedIn, YouTube, etc. has had a profound and transformational effect on activities ranging from commercial marketing to even the communication of official government information. Governments, from Prime Ministers, Presidents to local government officials, are using social media to communicate with their constituents. In 2015, there were more than 1.44 billion active monthly users of Facebook and 288 million Twitter users globally. One U.S. Congressman humorously summarized Twitter's virtues:

> "I know the overall importance of reaching out through the social media, because I have 31 grandchildren and they are on all of these things," said U.S. Rep. Buck McKeon, R-Calif. "This is mostly a young person's game and I'm an old person, but I'm young at heart ... the only advice I'd give is 'get involved' and then use it in the right way" (Sniderman 2011).

Social media presents government regulators with a host of issues ranging from privacy and cyber security to hijacking of computer systems (the latter concerns RATs, not the small furry types, but "remote administrative systems" that can remotely access and control computer technologies). Governments have responded to these social media risks in diverse ways. In Europe, concerns over individual privacy have promoted greater restrictions on social media providers. In the United States, there is no one overarching law that governs the actions of social media however there are myriad laws addressing diverse aspects of social media. These range from the Children's Online Privacy Protection Act (COPPA) to the Securities and Exchange Commission's concern (ultimately settled) over the use of Twitter by companies to announce forthcoming developments that might be in violation of U.S. law regarding the publication of market-sensitive information to the public.

5 Cloud Computing

One of the most important developments in digital technology has been the emergence of cloud computing for both the public and private sectors. In essence, cloud computing involves a large data center, which is typically managed by a third party, who holds and manages the client's information. Like an electric utility, data on the cloud is accessible by anyone, anywhere with access to the Internet and with the proper credentials. The advantages and potential offered by cloud computing are considerable: access to computer resources and data capacity at a cost far less than it would have to achieve if it used its financial resources. A computer executive aptly expounded on the potential that cloud computing services offer: "... an enterprise [can] expand its infrastructure, add capacity on demand, or outsource the whole infrastructure, resulting in greater flexibility, a wider choice of computing resources and significant cost savings" (Mohamed 2009).

While cloud computing technology offers enormous potential for expanding and improving government services, the cloud also presents a host of potential legal and regulatory issues:

- Establishes a new relationship between the owner of the information, its users, and the cloud provider—a third party relationship that creates a potentially complex set of governance issues, e.g. legal obligations for control of the information and adherence to regulatory obligations.
- As a global service, information may cross multiple governments each of whom may have their own regulations concerning privacy thus compounding the challenges for service providers and users. For example, both the European Union and United States have differing views on the nature of privacy and privacy protections provided.
- Privacy and security are the greatest challenges. By its very nature, cloud computing means that the physical infrastructure used to store information is shared among various users. How is sensitive information to be handled? Government agencies have used various strategies, from encryption to tokenization, to safeguard data; however, there still exists the threat of hacking and unauthorized third-party access to the cloud.

6 Mobile Devices

As never before, mobile devices (e.g. smartphones, tablets, iPads) provide consumers with access to e-mail, apps and video almost anytime and anywhere. A market research company (eMarketer 2014) reported that 4.55 billion people worldwide are expected to use a mobile phone in 2014. Between 2013 and 2017, mobile phone penetration will rise from 61.1 to 69.4 % of the global population.

Government regulations for mobile devices, esp. cell phones, have focused on several key issues:

- The oversight of mobile phone providers range from the technical (allocation of bandwidth, or smart phones have the ability to display emergency alerts, e.g. dangerous weather) to the terms and quality of customer service.
- Health and safety issues, e.g. concerns that radiofrequency energy (or radio waves) may be injurious to human health, and that mobile devices are distractions while driving. A number of states in the United States and EU member states have passed cell phone safety bills. In March 2014, Belgium passed a law that the specific absorption rate (SAR) has to be listed for every mobile phone sold. SARs are a measure of radio frequencies that may (or may not) cause brain cancer due to intensive use of a mobile phone.
- The transmission of sensitive information. As mobile devices are able to transmit and receive a greater range of information, concerns have been expressed about the safety and security of this information. Here are two examples:
  - The American banking regulator (Federal Deposit Insurance Corporation) warned that "security concerns present significant challenges for financial institutions providing mobile banking services, and each delivery channel [Text messaging/short message service (SMS), Mobile-enabled Internet browser, Mobile applications (apps)] poses unique risks for institutions and customers" (FDIC 2011).
  - ENISA (the European Union Agency for Network and Information Security) in a 2010 report on smartphone risks cited a number of potentially dangers. These risks included improper decommissioning of the phone without removing sensitive data, phishing, spyware that allows an attacker to access or infer personal data and surveillance of the targeted user's smartphones (Hogben and Dekker 2010).

7 Key Regulatory Challenges Facing Digital Government

While each component of digital government presents their own unique issues, there are six common areas that all digital governments will have to address. These areas pose significant challenges for digital government in that they touch on the most sensitive questions of national sovereignty, personal privacy, balancing national security and individual rights, protecting personal access to and transmittal of information, the challenges posed by the "internet of things", and governmental oversight and regulation in a rapidly changing governance environment.

8 Privacy

The vast collection of organizational and personal information by both public and private entities and the ability of new technologies to intrude into people's daily lives have prompted calls for greater vigilance and protection. Privacy covers a broad range of concerns: fears for the safety of children in chat rooms and on the Internet, the privacy of e-mail, the vulnerability of web users to having their Internet usage tracked, and the freedom of people to talk and post messages anonymously.

A 2012 report by the U.S. government entitled: "*Digital Government: Building a 21st Century Platform to Better Serve the American People*", expressed this concern:

> As the federal government builds for the future, it must do so in a safe and secure yet transparent and accountable manner. Architecting for openness and adopting new technologies have the potential to make devices and data vulnerable to malicious or accidental breaches of security and privacy. . . .moving forward we must strike a balance between the very real need to protect sensitive government and citizen assets given the realities of a rapidly changing technology landscape (Executive Office of the President of the United States 2012).

The United States is certainly not alone in this concern. Europe's desire to protect individual privacy is reflected in a 2014 ruling by the Court of Justice of the European Union in a Spanish case involving Google. The court stated the fundamental right of privacy "override[s], as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the [individual's] name." In response to this ruling, on May 29, 2014, Google launched its official request process for removing search results. From May 29, 2014, through Feb. 13, 2015, Google received 216,810 requests from individuals for removal of URLs from search results. These 216,810 requests addressed 783,510 different webpages. As a result of the official request process, 59.7 % of the webpages have been removed from Google's search results (Feldman 2015).

For digital government, the issues of privacy touch on a number of complex, important and sensitive issues for both public and private entities. What is a sufficient level of consent when collecting personal information online from the person providing the data and when does it have to be provided? When does a person decide to "opt in" or "opt out" of providing information? What steps will be taken to protect information? With the trans-national flow of information, digital government will have to formulate policies on the transfer of information outside its national boundaries to protect citizen privacy. For example, the EU has stringent requirements on transferring personal data outside the European Economic Area. Who may receive this information and under what circumstances poses substantial issues. And even cookies deserve special mention. New EU Internet privacy laws require website providers must obtain consent from visitors before storing or retrieving any information on a computer, smartphone or tablet.

For digital governments, the need to address privacy is critical. A citizen's daily life is affected by technologies that can track and record an individual's most routine activities. The choices are stark and complex: the quest to balance the rights, security and privacy of its citizenry with the enormous potential these new technologies offer governments to protect its own self-interests.

9 Cybersecurity

The threat of unauthorized access to the tools of digital government is a serious issue. A 2015 global survey by the Internet Society reported that 86 % of the respondents said that cybersecurity is the most important issue facing the Internet community today (ISOC 2015). Hacking has been a repeated threat to the Internet. Repeated stories of foreign intrusions into US government systems have proliferated. In 2009, President Obama bluntly said of this problem: "it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation" (Office of the Press Secretary 2009). Ranging from the North Korean hacking of Sony Pictures' email and digital information system in retaliation for a film it deemed offensive, to repeated stories of Russia and China hacking of US government systems,[3] including the President of the United State's private (unclassified) emails, In 2015, hackers attacked the German Bundestag lower house of parliament's computer system, and Chancellor Angela Merkel's mobile phone.

Other accounts[4] illustrate the scope and impact of cyber threats across the spectrum of digital technologies:

- In 2013, *Daily Mail* reported that security experts found a cache of two million pilfered passwords to popular social media websites including Facebook, Google, Twitter and Yahoo from Internet users across the globe. These included 326,000 Facebook accounts, 60,000 Google accounts, and more than 59,000 Yahoo accounts (Daily Mail Reporter 2013).

[3] In June and July, 2015 it was reported in various media that hackers had stolen a vast amount of data from the U.S. government's Office of Personnel Management (OPM) computer networks. It included information on 21.5 million people who had undergone background checks for security clearances. In a separate but related data breach, information on 4.2 million current and former U.S. workers were stolen. It was estimated that the total number of people affected by these actions represented almost 7 % of the U.S. population (Zengerie and Cassella 2015).

[4] In July 2015, the United States' National Highway Traffic Safety Administration was investigating a threat to the security of the Fiat Chrysler Jeep and a hacker being able to gain control over its dashboard connectivity system. A recall of 1.4 million cars was initiated to correct potential system flaws. One U.S. Congressman said of the issue, "cars today are essentially computers on wheels, and the last thing that drivers should have to worry about is some hacker along for the ride" (Kessler 2015).

- In April 2015, hackers acting in support of Islamic State extremists knocked out the global broadcast network of France's TV5, and then hijacked its website and social media to post warnings against French participation in air strikes against militants in Iraq and Syria.

To confront the need to protect against cyber threats, digital governments will have to consider a variety of measures to safeguard its citizens and assets. Given the nature of these threats, cybersecurity strategies must be interdisciplinary and comprise multiple stakeholders (public and private sectors, enhanced international cooperation). With these initiatives, digital government can improve its risk management capability to respond to vulnerabilities, threats, and fix potential weaknesses. These initiatives need to ensure that critical information infrastructures have the ability to prevent, detect and manage incidents, and that there is a coordinated response to incidents and recovery. Beyond strategy and policy, technology must be applied that can assist governments to monitor, collect and analyze information and identify patterns that indicate breaches or attempted breaches of cyber security. It is crucial that digital government have the trust and confidence of its citizens and institutions to protect the security of their information.

9.1 A Balancing Act

Yet in its quest to protect the security of information, digital governments must also respect the fundamental rights its citizens to freedom of speech and information. The OECD in its 2012 report on cybersecurity national strategies, *Cybersecurity Policy Making at a Turning Point*, remarked "all strategies place a strong emphasis on the need for cybersecurity policy to respect fundamental values, which generally include privacy, freedom of speech, and the free flow of information" (OECD 2012).

10 Control of Internet Content

With the extraordinary capabilities of the web, comes the equally extraordinary regulatory challenge presented by this global information device. Writing in the *Huffington Post*, a commentator said of the Internet: "[it] allows individuals and groups of individuals to speak directly to each other and to the world at large without the requirement or necessity of intermediaries moderating their content . . . To advocate or to disassociate with the collective views of other speakers, to associate locally and globally, and to allow for human creativity and innovation is unprecedented in history" (Brown 2015).

Yet this capability to share and disseminate information and ideas is not unlimited. Similar to other forms of telecommunications, nations have taken action to

regulate the use and content of the Internet, in such areas as privacy, national security information, child pornography. Control of Internet content reflects the cultural, religious, and political norms of the country. The diversity of prohibited speech can be staggering. For example, an ICANN official, pointed that "more than two-dozen countries, found everywhere from Western Europe to Asia to Africa, have laws or policies that penalize blasphemy" (Grogan 2015).

A growing number of governments have taken very restrictive measures to control Internet content. The *New York Times* reported in 2012 that the number of governments that censor Internet content has grown to 40 from about four in 2002 (Cerf 2012). In February 2014, the countries whose governments censored the most Internet content were North Korea, Myanmar, Cuba, Saudi Arabia, Iran, Syria, Tunisia, Vietnam and Turkmenistan (USA Today 2014). The Chinese has taken extreme proactive measures to control Internet content. It was reported that China has between 20,000 and 50,000 police to censor unwanted Internet content (Ken 2012).

10.1 Google and China

A classic example of the conflict between the Internet providers and government can be seen in the 2010 controversy that erupted between Google, the Internet search company, and China over the latter's desire to censor several of Google's features including its YouTube, search and email applications.

By way of background, China has taken a very stringent view of Internet content.[5] A 2010 White Paper issued by the State Council of the People's Republic of China issued a range of prohibitive items that included: "being against the cardinal principles set forth in the Constitution; endangering state security, divulging state secrets, spreading rumors, disrupting social order and stability, humiliating or slandering others." (Information Office of the State Council of the People's Republic of China 2010)

When Google initially launched its search engine site in January 2006 it had agreed to comply with the Chinese government's censorship laws and filter the site's search results. While Google was subject to considerable negative reaction to its accommodation with the Chinese government, it responded to the Chinese limitations by saying "While removing search results is inconsistent with Google's mission, providing no information (or a heavily degraded user experience that amounts to no information) is more inconsistent with our mission" (CNN.com, 2006).

[5]Since 2014, the Chinese government is using a broader interpretation of existing law to exercise stringent control over internet speech. As the New York Times reported, "Artists, essayists, lawyers, bloggers have been hauled into police stations and investigated or imprisoned for 'picking quarrels and provoking trouble'". The definition of picking quarrels now encompasses on-line activities. First time offenders can be sentenced up to 5 years in prison (Wong 2015).

However, in 2010, Google complained that it was the target of Chinese hacking operations (esp. with respect to human rights advocates), and it would no longer act in accordance with China's censorship laws. The Chinese government responded by blocking Google completely in Mainland China, but reversed the ban the following day. While Google still operates in China, it operates in compliance with the Chinese government's censorship requirements.

10.2 Other Examples

While China may be a dramatic example, other countries are not immune in seeking to control Internet content. Turkey has periodically censored Internet content. In 2015, the country banned access to Twitter and YouTube after images of a government prosecutor held hostage by militants were published. In 2014, the same networks were also blocked in advance of local elections. The government said that allegations of corruption by local officials were being shared online (Akkoc 2015). Russia, in August 2014, required all bloggers with 3000 daily readers to register with the country's Internet censor (Dewey 2015). The United States has taken controversial actions to access Internet information. It was revealed in 2013 that the United States' National Security Agency had secretly broken into the main communications links that connect Yahoo and Google data centers around the world. By its actions, the NSA could collect, at will, hundreds of millions of user accounts, many of them belonging to Americans (Gellman and Soltani 2013).

11 Ownership

Given the Internet's critical role in the future of digital government, a question keeps arising as to who "owns" the Internet. Regulation is only effective to the extent that there is an entity that can respond to the regulatory actions being mandated. In the case of Internet especially, the answer in a complex set of organizations (public, private and non-profit) and rules seeking to regulate technologies that often have no national boundaries. Indeed, reflecting the Internet's open and international operations, as well as its engineering origins, oversight of the Internet is split among a complicated structure of international and national governments, and self-regulating organizations, or "multi-stakeholders". The 2005 Tunis Agenda for an Information Society reflected this concept. It defined Internet governance as "the development and application by governments, the private sector and civil society, in carrying out their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of Internet." (World Summit on the Information Society 2015). Finally, there is the American origin of the Internet that has had enormous influence over Internet and the organizations that govern its operations.

As noted earlier, there are several key non-governmental organizations that oversee the technical global operations of the Internet. The Internet Engineering Task Force (The IETF) focuses on the myriad technical issues involved in Internet usage, such as Internet architecture, Hypertext Transfer protocols, and addressing operating and technical issues in the Internet. The second is the World Wide Web Consortium (W3C) that oversees the core standards and protocols of the Web. It is the third organization that is probably the most widely known, and controversial, the Internet Corporation for Assigned Names and Numbers (ICANN).

ICAAN's role is critical in the governance of the web. It is responsible for registering Website domain names and Internet Protocol (IP) addresses. The latter allows an email to reach its destination or for a web page to be sent to the right computer through the web. The controversy has centered about the American dominance of ICANN and encapsulates some of the concerns over the future governance of the Internet. ICAAN was originally created by the U.S. Department of Commerce to handle the technical tasks cited above. In March 2014, however, the U.S. government announced that it would end its long-running contract between the Commerce Department and ICANN, and open it to broader international management.[6] While one government official said, "[the move was] consistent with other efforts the U.S. and our allies are making to promote a free and open Internet, and to preserve and advance the current multi-stakeholder model of global Internet governance", others have a rather darker point of view. A former senior Congressional leader said, "What is the global Internet community that Obama wants to turn the Internet over to? This risks foreign dictatorships defining the Internet." (Timberg 2014)

Beyond the technical international governance of the Web, there is the growing role of the United Nations and one of its agencies, the International Telecommunications Union (ITU). Established in 1865 with the signing of the first International Telegraph Convention, the agency focuses on information and communication technologies. However, a 2012 World Conference on Information Technology (WCIT), hosted by the ITU, erupted in controversy as to the role of the ITU in Internet governance. It pitted country vs. country over governance issues and what the appropriate role of the ITU (if any) should be in this process.

In this conflict, the United States was adamantly opposed to the role of the United Nations in Internet governance. To illustrate this passion, the United States House of Representatives and the Obama administration (in a rare moment of joint agreement) opposed ceding any control of the Internet to the United Nations. A 2012 unanimous resolution by the House urged the Obama administration to fight efforts to give a United Nations agency control over the Internet. A member of congress said of the resolution, "Today's unanimous vote sends a clear and

[6]In August 2015 a draft proposal for the future governance of ICANN was published. Under the proposal, ICANN would be an independent entity without US government oversight and the transition would take place sometime in mid-2016. https://www.icann.org/en/system/files/files/ccwg-draft-2-proposal-work-stream-1-recs-03aug15-en.pdf

unmistakable message: the American people want to keep the Internet free from government control and prevent Russia, China and other nations from succeeding in giving the U.N. unprecedented power over Web content and infrastructure . . . we cannot let this happen." (Sasso 2012)

11.1 National Sovereignty and Net Neutrality

Governments have had a long history of regulating telecommunications within their national boundaries, and indeed often operating telecommunications systems themselves. A 2015 federal government decision in the United States perhaps illustrated the complexities facing national regulation. Up to that time, Internet service providers were subject to only limited federal government regulation. However, In November 2014, President Barack Obama asked the Federal Communications Commission (FCC) to implement regulations in the Internet sector comparable to those with respect to telephones. One of the goals was to prohibit broadband companies, such as Verizon and Comcast, from favoring some providers of Internet services or online media sources over others. Of this issue, President Obama was quite adamant, "I personally, [and] the position of my administration, . . . is that you don't want to start getting a differentiation in how accessible the Internet is to different users. You want to leave it open so the next Google and the next Facebook can succeed." (Obama 2014) Thus Obama succinctly framed the concept of "net neutrality". All data on the Internet deserve equal treatment by enterprises, including Internet service providers, and by governments. Major telecommunications providers who, among other concerns, feared not being able to charge different prices for different classes of Internet access met it with enormous opposition.

In February 2015, the FCC ruled in favor of net neutrality. The resultant reaction was vehement. The *Washington Post* noted of the decision that "It's not an exaggeration to say that this marks a turning point in the history of the Internet" (Fung 2015). Upon its passage, the FCC unequivocally stated, "The FCC's Open Internet rules protect and maintain open, uninhibited access to legal online content without broadband Internet access providers being allowed to block, impair, or establish fast/slow lanes to lawful content" (NewsOK 2015). Not unexpectedly industry reaction was not as enthusiastic. A telecommunications industry representative direly warned that ". . . now that it is a telecommunications service, it is by definition subject to the international treaty governing telecommunications." (Wilson 2015)

11.2 The Growing Debate Over Net Neutrality

The issue of net neutrality is not limited to the United State. In 2015, the European Council, which is made up of the 28 national governments of European Union

members, voted in favor of changing the rules to bar discrimination in Internet access but allowing the prioritization of some "specialized" services that required high quality Internet access to function. This is in contrast to the 2014 vote by the European Parliament that endorsed net neutrality (Geere 2015). India also is currently debating the virtues or faults of allowing some telecommunication companies to charge fees for faster access to the Internet (Soni 2015).

12 The Internet of Things and Big Data

The dramatic evolution of digital technology and its impact on both individual and corporate life is reflected in the concept of the 'Internet of Things" (IoT), This term, coined by Kevin Ashton in 1999, is used to describe embedded devices (things) with Internet connectivity, allowing them to interact with each other, services, and people on a global scale. Through the use of radio-frequency identification (RFID) tags and other types of sensors planted inside a physical object it gives it the power to be monitored and controlled remotely through the Internet. This connectivity is reflected in appliance ranging from smart watches to home thermostats, security systems, and even traffic lights. In 2014, the Gartner research organization forecasted that "4.9 billion connected things will be in use in 2015, up 30 % from 2014, and will reach 25 billion by 2020... the IoT has become a powerful force for business transformation, and its disruptive impact will be felt across all industries and all areas of society." (Gartner 2014)

This capability also has the ability to generate enormous sums of information ("big data"), both structured and unstructured, that can be used in an infinite variety of uses.[7] A German report succulently reported on the potential (and risks) for "smart products" that have embedded Internet connectivity devices: "Once they have left the factory, smart products are connected via the Internet. They exchange ever-larger volumes of data during use. It could be argued that these mountains of data (big data) actually constitute the most important raw material of the twenty-first century" (Acatech 2015).

12.1 Implications for Regulation

For digital government, this technology presents significant opportunities to improve and expand government service e.g. from enhanced health care to traffic

[7]On March 27, 2014, AT&T, Cisco, GE, IBM and Intel announced that they were forming the Industrial Internet Consortium (IIC), an open membership group to support better access to big data with improved integration of the physical and digital worlds (Industrial Internet Consortium 2014).

management, it also faces critical regulatory challenges and risks (the "disruptive impact" mentioned above) in a number of areas including data security and privacy, and intellectual property protection.[8] For example:

- Developing a policy framework to protect individual privacy. In a report commissioned by the President of the United States in 2014 on big data, the advisory panel cautioned ". . . how to balance the socially beneficial uses of big data with the harms to privacy and other values that can result in a world where more data is inevitably collected about more things" (Council of Advisors on Science and Technology). For example, how should the Fair Information Practice Principles ("FIPPs"), which include notice, choice, access, accuracy, data minimization, security, and accountability provisions, apply to the IoT? How do the geographic and political boundaries for data protection, such as in the EU, influence the use of big data? How do countries provide uniform standards for data protection and privacy?
- The essence of big data's potential is that it can be shared among various parties. This includes the sharing of the means of creation, compilation and analyses of the data. The challenge for big data and business falls into three key areas: patents, trade secrets, and copyright. The issues are daunting. A legal expert writing on the topic said, " . . . Intellectual property rights—who owns the input data companies are using in their analysis and who owns the output—in big data technologies are at least as important as data privacy issues which have perhaps been more widely reported." (Out-Law.com 2013). The legal questions pose unique and challenging problems for organizations, for example, how do governments harmonize copyright protections or can algorithms used to analyze the data be legally protected?

13 Regulatory Practices and Challenges

Transcending all the regulations cited above is the challenge that digital governments will confront in devising policies, rules and regulation in a dramatically changed environment. As mentioned earlier in the chapter (p. 3), in a world shaped by the desire to have "information-centric, mobile enabled and collaborative digital environments" government administrators will have to re-evaluate many of the traditional methods of rule making for a new reality. Change is a theme that is cited by proponents of digital government. Arnis Dauglis, the chief information officer of Lativa and a leading proponent of digital government, said of the transformative

[8] In 2015, the United States' Federal Trade Commission created the Office of Technology Research and Investigation (OTIR) to research issues on technology's impact on consumers including privacy, data security, connected cars, smart homes, algorithmic transparency, emerging payment methods, big data, and the Internet of Things.
https://www.ftc.gov/news-events/blogs/techftc/2015/03/booting-new-research-office-ftc

impact of digital technology on government operations, "... it is much more about change than technology—change of the mindset and skill set of public sector officials, change of business processes, of making public services user-friendly and accessible. If governments are really committed to the digital agenda, they should be committed to the above-mentioned changes. Otherwise they are cheating themselves and their people." (Dauglis 2014)

Change will have a profound impact on many of the issues confronting governance of the new digital government.

- What should be the structure and process for regulating these new technologies? Traditional methods of government control will have to be reformulated for technologies that have no national boundaries. The current "multi-stakeholders" process of using national and regional governments, non-profit private organizations to regulate the Internet may ultimately present the most pragmatic strategic direction. The question is always, "who owns the Internet" and how should it be managed in a country's self-interest.
- The balance of national sovereignty and "internationalization" of the Internet will be a major challenge. The desire of government to have greater control over Internet governance, from setting technical standards to the control of access and means of communication will shape the regulatory environment for digital governments.
- In creating a more collaborative form of government, how will regulations be developed and managed in a digital environment. An example is the introduction of "e-rulemaking" in the U.S. government. As part of its regulatory process, an on-line system is available for the public to comment on proposed regulations. It allows electronic participation in a process that until recently was largely prohibitive for the general public. A George Mason University report (Brito 2010) talked of a potential 'second generation" of e-rulemaking that would use social media, such as Facebook and Twitter and collaborative commenting systems, to enhance citizen participation in governance.
- With the increasing importance of digital tools in providing government services, a question arises as to whether its use should be made mandatory. This raises difficult problems for citizens who neither have access to the Internet nor adequate knowledge to use it. A British report (Chatfeld 2014) on the issue recommended "a caring system that accommodates people and does not force technology upon them".
- The speed of technological change is daunting. The ability of governments to regulate technologies that may be outdated by the time the usual regulatory process has been completed will be a major issue. Equally challenging for digital governments will be finding the technical expertise to understand and manage these technologies. The lure of private sector organizations, with more pay and other benefits, can be a major problem in recruiting staff with the requisite technical knowledge to lead the new digital government. The complexities of new technologies will be a major issue for governments to deal with unless it has the knowledge and expertise to fully understand the capabilities and limitations

of these technologies, and the willingness to adopt new management styles, such as the "agile" project development methodology used in technology organizations.

- How will digital government address the difficult issue of citizen privacy? The White House report published in May 2014 (Council of Advisors on Science and Technology) elegantly expressed the concern of new technologies being able to "pierce many spaces that were previously private." For the digital government, being able to balance its security needs with the right of individuals to not only have freedom of speech and access to information, but be protected from intrusion into their daily lives, will be a continuing challenge.
- Similarly, how does digital government address the emerging and complex issues of big data and the Internet of things? Challenges to privacy, intellectual property, data security pose daunting issues that government will have to confront.[9] The issues, as noted in the footnote below, are compounded by the early stage of technological development and the regulatory, legal and legislative strategies that need to be adopted.

14 Conclusion

The promise of digital government is extraordinary but challenging. The tools of digital government: Internet, cloud computing, social media, mobile devices, big data are incredible in their power to inform and transform. Indeed the future of the Internet is likely a convergence of these technologies. Never in human history have we had the ability to communicate on a global scale with a speed that transforms distant events into immediate concerns.

14.1 The Road Ahead

Yet, there are also major concerns for regulatory management by government. As we have seen, many of the traditional methods of government regulation are being challenged by these new technologies. This situation is acerbated by the fragmented, borderless, and mobile characteristics of these technologies that make defining a particular course of action, or object of a regulation extremely

[9]In a workshop hosted by the US Federal Trade Commission in 2013 on IoT), participants urged caution in regulatory actions. One participant noted that "we should be careful to kind of strike a balance between guiding companies in the right direction and enforcing". Another participant feared that the workshop "represents the beginning of a regulatory regime for a new set of information technologies that are still in their infancy" https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

difficult, at best. Writing in the *Harvard Journal of Law & Technology*, Kevin Werbach framed the issue: "the key challenge for the evolving Internet ecosystem is not competition, but cooperation. All participants in the market . . . participate in the same interconnected network of networks. The fundamental technical and economic question is how they can act independently, pursuing their own private ends, while still contributing to the health and stability of the global mesh"(Werbach 2009). For digital government how can it manage this "global mesh" to protect fundamental rights without hindering the growth of vital technologies, and yet ensure the stability of this multi-dimensional entity. How does the often laborious, fragmented framework and process for regulatory decision-making address this situation?

As digital government confronts these issues, it has several important strategic regulatory directions that it may consider:

- Maintain a traditional nationalist approach that adopts country law to the global network of information and technology. While it can address such country-specific issues as net neutrality or Internet content, it is often legally powerless to control technologies beyond its jurisdiction.
- Adopt either a regional or global approach to regulation. In the same 2015 survey by the Internet Society cited earlier in the chapter (p. 11), respondents suggested using regional entities, such as AfTLD (African Top Level Domain), to address country issues with the Internet and set regional standards. The EU is working on the creation of a Single Digital Market by 2020 to address similar issues. On a global level, non-governmental entities, e.g. World Wide Web Consortium (W3C) and ICANN continue to set standards for Internet operations. The UN and the ITU may ultimately play a key global role in Internet management. While these approaches address trans-national digital concerns, the need for individual countries to harmonize their national laws, or even agree to these regulations, is often a long, tedious process.
- Utilize a broad range of regulatory schemes, both nationally and internationally, to address the issue of public and private management of these technologies. No one single approach will be adequate. An eclectic combination of self-regulation, co-regulation, public-private partnerships, and international (or regional) standards setting and enforcement may ultimately be the most practical and pragmatic approach to addressing the challenges faced by digital government.

References

Acatech (National Academy of Science and Engineering). (2015). Smart service welt: Recommendations for the strategic initiative web-based services for business. http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Projekte/Laufende_Projekte/Smart_Service_Welt/BerichtSmartService_engl.pdf

Akkoc, R. (2015, April). Turkey blocks access to social media and YouTube over hostage photos. *The Telegraph*. http://www.telegraph.co.uk/news/worldnews/europe/turkey/11518004/Turkey-blocks-access-to-Facebook-Twitter-and-YouTube.html

Brito, J. (2010). The promise and limits of E-Rulemaking. *Mercatus Research*. http://mercatus.org/sites/default/files/publication/promise-and-limits-of-e-rulemaking_1.pdf

Brown, K. (2015). A ray of light shines on internet rights. *The Blog*. http://www.huffingtonpost.com/kathy-brown/a-ray-of-light-shines-on-_b_7026544.html

Cerf, V. G. (2012, May 24). Keep the internet open. *The New York Times*. http://www.nytimes.com/2012/05/25/opinion/keep-the-internet-open.html?_r=0

Chatfeld, T. (2014). Making digital government work for everyone. *Digital Government Review*. http://digitalgovernmentreview.readandcomment.com/wp-content/uploads/2014/11/EMBARGOED_CONFIDENTIAL_MASTER-Final-Report-20141124_CLEAN.pdf

CNN.com Google to censor itself in China. (2006). http://www.cnn.com/2006/BUSINESS/01/25/google.china/

Council of Advisors on Science and Technology. (2014). *Big data and privacy: A technological perspective*. https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_amr_sept_2014_final.pdf

Daily Mail Reporter. (2013, December 4). Hackers steal usernames and passwords for TWO MILLION social media accounts—and many of the log-ins were as easy as '123'. http://www.dailymail.co.uk/news/article-2518540/Facebook-Twitter-hackers-steal-passwords-2m-social-media-accounts.html

Dauglis, A. (2014). How digital technology can drive modernisation throughout government. *Delivering Public Service for the Future*. www.lisboncouncil.net/index.php?option=com_downloads&id=1070

Dewey, C. (2015, April 10). Russia just made a ton of mems illegal. *Washington Post*. Accessed July 27, 2015, from https://www.washingtonpost.com/news/the-intersect/wp/2015/04/10/russia-just-made-a-ton-of-internet-memes-illegal/

eMarketer. (2014). Smartphone users worldwide will total 1.75 billion in 2014. http://www.emarketer.com/Article/Smartphone-Users-Worldwide-Will-Total-175-Billion-2014/1010536

Executive Office of the President of the United States. (2012). *Digital government: Building a 21st century platform to better serve the American people*. https://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html

FDIC. (2011). Mobile banking: Rewards and risks. *Supervisory Insights*. https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin11/mobile.html

Feldman, J. (2015). Internet indelibility and the right to be forgotten. *Daily Report*. http://www.dailyreportonline.com/id=1202725862358/Internet-Indelibility-and-the-Right-to-Be-Forgotten

Fung, B. (2015). Your guide to net neutrality: Everything you need to know about today's FCC vote. *The Washington Post*. https://www.washingtonpost.com/blogs/the-switch/wp/2015/02/26/your-guide-to-net-neutrality-everything-you-need-to-know-about-todays-fcc-vote/

Gartner. (2014, November 11). Says 4.9 billion connected "things" will be in use in 2015. http://www.gartner.com/newsroom/id/2905717

Geere, D. (2015, March 7). Europe reverses course on net neutrality legislation. *Ars Technica*. http://arstechnica.com/business/2015/03/europe-reverses-course-on-net-neutrality-legislation/

Gellman, B., & Soltani, A. (2013, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Grogan, A. R. (2015). ICANN is not the internet content police. *ICANN Blog*. https://www.icann.org/news/blog/icann-is-not-the-internet-content-police

Hogben, G., & Dekker, M. (2010). *European Network and Information Security Agency (ENISA)*. Smartphones: Information security risks, opportunities and recommendations for users.

Industrial Internet Consortium. (2014). AT&T, CISCO, GE, IBM and INTEL form industrial internet consortium to improve integration of the physical and digital Worlds tech. http://www.iiconsortium.org/press-room/03-27-14.htm

Information Office of the State Council of the People's Republic of China. (2010). The Internet in China. http://china.org.cn/government/whitepaper/node_7093508.htl

Internet Society (ISOC). (2015). *Internet Governance Survey 2015*. http://www.internetsociety.org/doc/internet-governance-survey-2015

ITU. (2014). *ITU releases 2014 ICT figures*. http://www.itu.int/net/pressoffice/press_releases/2014/23.aspx#.U2pey2RdVz1

Ken, M. (2012). Protests, not criticism, the target for China's internet censors, study says. *PCWorld*. http://www.pcworld.com/article/257707/protests_not_criticism_the_target_for_chinas_internet_censors_study_says.html

Kessler, A. M. (2015, July 25). Fiat Chrysler issues recall on hacking. *New York Times*.

Mohamed, A. (2009). A history of cloud computing. *Computerweekly.com*. http://www.computerweekly.com/feature/A-history-of-cloud-computing

NewsOK. (2015). Will 'net neutrality' make access fair for customers, or stifle growth? http://newsok.com/will-net-neutrality-make-access-fair-for-customers-or-stifle-growth/article/feed/812544

Obama, B. (2014). Net neutrality. https://www.whitehouse.gov/net-neutrality

OECD. (2012). *Cybersecurity policy making at a turning point*. http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Office of the Press Secretary, the White House. (2009, May). Remarks by the President on Securing Our Nation's Cyber Infrastructure. https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

Out-Law.com (Pineset Masons). (2013). Big data: Privacy concerns stealing the headlines but IP issues of equal importance to businesses, says expert. http://www.out-law.com/en/articles/2013/march/big-data-privacy-concerns-stealing-the-headlines-but-ip-issues-of-equal-importance-to-businesses-says-expert/

Sasso, B. (2012, August 2). House urges Obama to fight UN web regulation. *The Hill*. http://thehill.com/policy/technology/242007-house-urges-obama-to-fight-un-internet-regulation-in-unanimous-vote

Scholl, A. (2012). The problem with internet regulation. *World Policy Blog*. http://www.worldpolicy.org/blog/2012/09/25/problem-internet-regulation

Silverman, M. (2008). *Compliance management for public, private or nonprofit organizations*. New York: McGraw-Hill.

Sniderman, Z. (2011). How governments are using social media for better and for worse. *Mashable*. http://mashable.com/2011/07/25/government-social-media/

Soni, A. (2015). How people power took on big business in the fight for net neutrality in India. *The Guardian*. http://www.theguardian.com/technology/2015/may/25/india-net-neutrality-people-power

Timberg, C. (2014). U.S. to relinquish remaining control over the Internet. *The Washington Post*. http://www.washingtonpost.com/business/technology/us-to-relinquish-remaining-control-over-the-internet/2014/03/14/0c7472d0-abb5-11e3-adbc-888c8010c799_story.htm

USA Today. (2014). Top 10 Internet-censored countries. http://www.usatoday.com/story/news/world/2014/02/05/top-ten-internet-censors/5222385/

Werbach, K. (2009, Fall). Higher standards regulation in the network age. *Harvard Journal of Law and Technology, 23*(1).

Wilson, C. (2015). US Telecom: FCC's move has global implications. http://www.lightreading.com/net-neutrality/us-telecom-fccs-move-has-global-implications/d/d-id/714049

Wong, E. (2015, July 27). In War on Internet 'Troublemakers', China turns to law on picking quarrels. *New York Times*.

World Summit on the Information Society. (2015). Tunis agenda for the information society. http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

Zengerle Patricia and Megan Cassella. (2015, July 9). Millions more Americans hit by government personnel data hack. *Reuters*. http://www.reuters.com/article/2015/07/09/us-cybersecurity-usa-idUSKCN0PJ2M420150709