Hearing before the
Committee on Commerce, Science, and Transportation
Subcommittee on Communications, Technology, Innovation, and the Internet

"The Internet and Digital Communications: Examining the Impact of Global Internet Governance"
July 31st, 2018

The Honorable Michael Chertoff
Former Secretary of Homeland Security 2005-2009
Co-Founder and Executive Chairman, The Chertoff Group

Introduction

As we are all aware, the internet knows no borders. National sovereignty and borders, key elements of how those of us in the West have looked at legal and political issues since the Peace of Westphalia, lack their traditional meaning in a digital world in which data moves between servers and users without regard for their location or nationality. I can just as easily access my email in Geneva as I can in Washington. My service provider can seamlessly move my data between data centers in dozens of countries, with the decision to do so made by an algorithm. In some instances, a provider may not even know the physical location of the data, the underlying ones and zeros, or may "shard" the data, spreading it across multiple locations.

In this environment, it is nearly impossible for any one country to claim sovereignty over "their portion" of the internet. A country may have jurisdiction over the physical infrastructure of the internet within their country, but it cannot control the infrastructure beyond its borders nor can it control the services and offerings of providers in other countries. Practically speaking, the only way to truly control the internet within your country is to disconnect it from the rest of the world, as Russia recently threatened to do and as North Korea has done for much of its domestic population (leaving aside the activities of the country's cyber warriors).[1] Even China's Great Firewall, a costly but reasonably effective means of control, is unable to completely stem the flow of information deemed objectionable by the Chinese Communist Party to citizens within its borders.

More importantly, taking such drastic action comes at a significant cost. The internet is now a vital part of the U.S. and the global economies. In 2016 e-commerce sales in the U.S. totaled approximately $400B, or roughly 10% of all retail sales.[2] Mobile and internet banking use in the U.S. has also exploded, resulting in 2.5B bill-payment transactions in 2012 alone.[3] Beyond these transactions are entire companies built on the power of the internet, such as Google and Facebook. The internet has also fostered entirely new segments of the economy, such as ride and home sharing.

Beyond the economics, the internet serves as a massive, if imperfect, laboratory for democracy and free speech, allowing for the free exchange of ideas and information between all users regardless of nationality, location, or class. It has also allowed for large scale collaboration, resulting in the creation of the world's largest encyclopedia, Wikipedia, and various crowdfunding sites that allow individuals to raise funds for their ventures beyond the traditional confines of banks and institutional investors. On the darker side of things, the internet has also given

[1] *See* https://www.theregister.co.uk/2017/12/01/russia_own_internet/, https://www.scmp.com/news/asia/east-asia/article/2119146/how-north-korea-slowly-embracing-its-own-sealed-version-internet
[2] *See* https://www.census.gov/newsroom/press-releases/2018/estats-report.html
[3] *See* https://www.frbservices.org/assets/news/research/2013-fed-res-paymt-study-summary-rpt.pdf

rise to a dark web that facilitates the sale of illicit goods and gives opportunities to criminals to conspire and collaborate in private.

Need for coordinated action on cyber (international and bilateral)

The internet has proven to be a vital economic and social tool, vastly expanding economic opportunity while allowing for the free exchange of thoughts and ideas. It is something that is worth protecting, but also something that requires regulation and policing. However, this global nature also necessitates an appreciation that the actions of one country can have impacts far beyond that country's borders, and conversely, that broader internet and cyber policy aims can only be fulfilled through cooperation with other countries.

That said, we must recognize that not all countries view the internet in the same way nor appreciate its significant social and democratic value to society. China, Russia, Iran, and many other authoritarian countries view the internet as a threat to the governing regime and thus require significant controls and monitoring. In such countries various websites are blocked, applications prohibited, and communications monitored for seditious speech or efforts that might challenge the regime's hold on power. While these countries are part of the global network, the reality is that we are never going to see eye-to-eye with them on important issues of internet governance, nor will the U.S. and its allies be able to convince them to abandon their efforts and allow unfettered access to materials that might undermine them.

And so, it is up to us to cooperate and build consensus with like-minded countries, other democracies and Western countries who agree on the broader principles of the internet but may disagree about how to regulate, shape, and manage it. We must recognize that we may, at times, disagree with even our closest allies on policy particulars, but in the end, it is better to reach an imperfect compromise with them than allow for the disintegration of the internet as we know. So much of the internet's value is in its global nature, and we must work across international borders if we hope to preserve it as a common good.

Without that cooperation we are likely to see new barriers, intended or not, appear and impede the development and growth of the internet. Data localization requirements, for example, may be enacted to protect a country's citizens' data, but have the more practical effect of significantly raising costs, diminishing competition, frustrating international commerce, and preventing citizens from accessing the services of providers based outside their own country. New regulations may be enacted to protect users' privacy but result in unexpected delays in cross-border law enforcement cooperation. The best way to avoid such barriers is to work with other countries to address these issues, as many countries share the same concerns and would all benefit from coordinated action.

At present, the mechanisms for such cooperation are limited. Broader international bodies, such as the United Nations and International Telecommunications Union, include stakeholders from authoritarian countries which may use those bodies to pursue policies contrary to our vision for the internet. The European Union has arguably been the most successful multi-national body on this issue, developing Europe-wide policies such as the General Data Protection Regulation (GDPR). Some progress has also been made on bi-lateral solutions, such as the law enforcement data sharing agreements authorized by the recently enacted Clarifying Lawful Overseas Use of Data (CLOUD) Act, which allows for the U.S. to enter into bi-lateral, reciprocal law enforcement data access agreements with countries that meet a specified set of legal and human rights criteria. The first such agreement, between the U.S. and the U.K., is currently working its way through the approval process.

A variety of other organizations have also worked to address these issues. The Global Commission on Internet Governance and the Global Commission on Stability in Cyberspace, on which I have served, work to counter the fragmentation of the internet and offer guidance to policy makers seeking to address internet governance issues.[4] Toomas Hendrik Ilves, the former President of Estonia and Visiting Fellow at the Hoover Institution at Stanford University, recently proposed what he termed a new "Cyber NATO," a coalition of liberal democracies that is better able to meet the ubiquity of cyber threats and ensure proper, adequate response.[5] The President of Microsoft, Brad Smith, has proposed what he has dubbed a "Digital Geneva Convention," which outlines the rules of cyberspace and protects civilians and other bystanders from the offensive cyber activities of nation-states.[6]

The above is just a brief snapshot of the need for international cooperation on internet governance, be it multi-lateral or bi-lateral. Ultimately, the U.S. will be best served by working with countries that share its values and vision for the internet to find a mutually-agreeable approach to the myriad of privacy, security, regulatory, and management issues that face the internet as we know it. The U.S. would also be well served to consult with key stakeholders throughout the process, considering the concerns of the technology industry, the privacy community, and other actors as it develops its strategy for international engagement cooperation on internet governance and related cybersecurity issues. The costs of non-cooperation would be severe and ultimately harm the U.S., and the rest of the world, economically and socially.

Privacy needs and the impacts of inaction

Today's rampant technology, and the convenience and opportunity it offers, has numbed us to our loss of privacy. The availability of data is only going to grow in years and decades to come and we urgently need to regulate how government and the private sector can make use of that information. The creaky and dated legal framework that currently governs the collection and use of personal data was created decades ago when phone records and photographs constituted metadata. The U.S. needs a legal and policy structure built for the way the 21st century uses data—one that retains security and economic benefits without sacrificing Americans' liberty and civic values.

Privacy as we know it has been forever at least substantially lost, and the collection of data will—and must, for security reasons—expand. What must be preserved, however, by new laws and regulations is our autonomy—the ability to make our own personal choices restricted only by transparent laws and social norms, and to have a reasonable degree of ownership and control over the data we generate.

In March of this year, news broke that Cambridge Analytica was regularly harvesting our data for the purposes of manipulating American voters in favor of the Trump Campaign in 2016.[7] The entering wedge of Cambridge Analytica's data collection was an apparently limited request by a developer to have Facebook users complete an online survey. Slightly over a quarter of a million did so. But by downloading the survey, they opened the door to collection of data about all their friends and their other on-line interactions. As a result, data relating to approximately 50 million individuals was captured. Most of these people did not know that their information was being used. Perhaps improperly, this data was transferred to Cambridge to applying machine learning algorithms to correlate granular connections between individuals and their likely political predilections and interests. This analysis could then be applied for precisely targeted, individually focused political advertising aimed at potential voters. It is debatable whether this had an impact on the election outcome, but it is certain that political campaigns and even governments will continue efforts to refine and apply the political marketing techniques.

[4] *See* https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf

[5] *See* https://berlinpolicyjournal.com/a-digital-defense-alliance/

[6] *See* https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

[7] *See* https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html

And the purpose of those techniques will not only be to affect elections. As we have seen, information from Russia and other foreign powers has been used to create social division, sow public distrust, and even foment unrest. Weaponized data is the newest tool in the armory of subversion.

What all this illustrates, is that personal data has become one of the most valuable assets of the modern age. That is evident from the fact that many of the companies with the highest market capitalization are essentially earning revenue from data adapted to commercial marketing. But the value of these data assets increasingly also lies in their utility as a tool to drive political behavior, impact social stability, and even affect national security.

Even more significant, the business of aggregating and reselling an individual's data from multiple sources — social media, online searches, consumer purchases, and locational data — means that people will increasingly be subject to pressure to change their behavior from multiple sources: employers, insurers and governments. By way of example, China has embarked on a "social credit" plan to aggregate myriad data points of online and offline behavior, and award individuals a "score" that will affect their life prospects.[8]

For all of us what this means is that all the data we generate has become as valuable, and as worthy of safeguarding, as our money in the bank. Privacy — in the sense of shielding data from others — has been frayed given how easily third parties can collect and fuse our data. What must be protected now is our freedom of action, which requires that we take greater ownership and control of our data even when it is accessible to others.

Data security regulation & policy solutions

Part of the remedy will be adaptations in the law and regulation, changes that must allow for innovation but also the need to protect individuals from having their data abused or weaponized. When user data is collected by a platform to improve the user experience, consent should be readily presumed. But when the data is being used for other commercial purposes, or transferred to third parties, the law should mandate that the proposed new use of this data be clearly explained to the user, and the user's affirmative approval should be required. Opting in or out of this kind of data sharing should always be the user's choice and should not be the result of pressure or deception. Finally, platforms should be required to describe and make available to the user all the types of data being collected about him or her.

But the remedy also requires each of us becoming mindful of how and when we share our data. Sometimes that means we should not share data, or that we should pay for an online service instead of accepting a "free" benefit that we pay for with our personal information. We should also be careful about completing online surveys because the data we enter could wind up in different hands than we expect. Even more critical, we should consider that our online communications with friends may be harvested if those friends agree to grant access to their data. Finally, we must educate ourselves about the way data can be used to influence us, and to train ourselves to evaluate these messages critically.

Some data regulation had already progressed both abroad and at the state level. Under the GDPR, EU citizens have a right to know what's being done with their data, and a right to access it. GDPR requires any company doing business in the EU that interacts with and processes data of people in the EU to get explicit consent from users for every possible use to their data. Users will have a right to be "forgotten;" as in being able to request that a company delete their data, stop sharing it and force third-party firms from using it as well.[9]

[8] *See* https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4

[9] *See* https://www.lawfareblog.com/summary-eu-general-data-protection-regulation

In June of this year, California recently passed one of the toughest data privacy laws in the country, the California Consumer Privacy Act of 2018, impacting how businesses will be required to disclose the types of data that they collect, as well as allow consumers to opt out of having their data sold.[10] The legislation, which is similar to Europe's new GDPR protections, gives consumers more control over their personal data. It grants them the right to know what information companies like Facebook and Google are collecting, why they are collecting it, and who they are sharing it with. Consumers will have the option of barring tech companies from selling their data, and children under 16 must opt into allowing them to even collect their information at all.

While the legislation is a positive step forward for consumers' privacy, I acknowledge that addressing privacy through dozens or hundreds of regulations various states and cities would be unworkable, and that their needs to be a broader solution at the national and global levels. However, the country or state that takes the most action and has critical mass will ultimately have the most impact. Take the California Emissions Standards legislation as an example. Automakers were compelled to more or less follow those standards nationally once the automakers in the region were forced to comply with a higher level of emission standards than the federal requirement. To date, 12 states and the District of Columbia follow the California standards. Similarly, the jurisdictions that lead on data privacy legislation and impact most U.S. companies could effectively set the national standard.

Defending against disinformation across Western democracies and election interference

Attacks on democracy will affect all parties. If we want to establish concrete solutions, we need to exchange knowledge and take global-minded actions. Organizations like the Transatlantic Commission on Election Security, for which I am the co-chairman, focus on finding solutions to three major election meddling strategies: manipulation of social media, tampering with social infrastructure and leaking confidential documents. Working with political and private sector leaders, traditional and new media actors, and non- governmental organizations, the Commission promotes transatlantic coordination, identifying and plugging gaps and raising awareness of this important issue. It will also investigate the level of risk exposure across Western countries and provide concrete recommendations to address this problem head on.

A positive step forward are private sector initiatives like Microsoft's "Defending Democracy" initiative (with which I work). This initiative engages with stakeholders in democratic countries globally to protect campaigns from hacking through:

- increased cyber resilience measures, enhanced account monitoring and incident response capabilities;
- increased political advertising transparency online by supporting relevant legislative proposals such as the Honest Ads Act and adopting additional self-regulatory measures across our platforms;
- technological solutions to preserve and protect electoral processes and engage with federal, state and local officials to identify and remediate cyber threats;
- defending against disinformation campaigns in partnership with leading academic institutions and think tanks dedicated to countering state-sponsored computational propaganda and junk news.

Information Sharing

Cybersecurity information sharing, that is, the sharing of threat data, indicators, Tactics, Techniques, and Procedures (TTPs), and other data, is vital to helping others detect and prevent a cyber-attack. What makes information sharing so important is the fact that our cyber infrastructure is so diffuse. While one entity, such as

[10] *See* https://www.theverge.com/2018/6/28/17509720/california-consumer-privacy-act-legislation-law-vote

the FBI, Google, or Microsoft, may be aware of a particular vulnerability or threat, it can take days, weeks, or even months before the relevant information spreads throughout the cyber ecosystem and results in the deployment of patches, installation of new technologies, changes in network architecture, or the adoption of new policies that adequately counter the threat. Such information sharing is likely the most mature within the Federal Government, where agencies, particularly within the Intelligence and Defense communities, share vital information with one another to protect federal networks.

The good news is that information sharing efforts are also growing within the private sector of the United States, though much can still be done. Some of the greatest progress has been made through the growth and use of Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs), which coordinate the sharing of threat information among entities from a single sector or geographic region. Some of the most successful ISACs and ISAOs, including the Financial Sector ISAC (FS-ISAC) and the Multi-State ISAC (MS-ISAC), have been able to coordinate the sharing of significant volumes of threat information between private and public entities while working with federal agencies to ensure that the threat information that they are able to provide is also reflected within their ecosystem.

However, more can be done to grow information sharing beyond the government space and a relatively limited portion of the private sector. First, the Federal Government can do more to encourage private sector information sharing both by enhancing incentives for private sector companies to participate and by making it easier for those companies to access threat information data from federal agencies.

Second, at present, information sharing across international borders is exceedingly difficult. Unclear data privacy requirements, data transfer limitations, and other legal uncertainties often prevent or significantly delay the sharing of threat information data between private entities in different countries. The United States should work with its international partners to help ease these restrictions while maintaining and respecting relevant privacy protections for sensitive personally identifiable information.

Third, international information sharing between governments can also be enhanced. While cooperation between U.S. intelligence agencies and those of our allies is generally effective, such cooperation is far less common between civilian agencies, sometimes because of the same regulations that frustrate private sector information sharing across international borders. We can do more to enable this information sharing and build stronger relationships between the Department of Homeland Security, which is responsible for the protection of federal civilian networks, and its counterparts in allied countries.

Five Frameworks for New Laws and Rules to Enhance Security and Civil Liberties

Finally, I would offer this committee and their colleagues in Congress five frameworks that they should contemplate as they consider how best to address the cyber threats facing our country and the policy challenges that those threats and changing technologies present. While no one framework is a silver bullet for the challenges we face, each helps to illustrate both these challenges and some of the specific solutions that could address them.

First, to protect us against attacks on our physical and cyber security by bad actors while simultaneously preventing the government from overreaching to threaten our autonomy, we must recognize that data requires both a loosening on what information can be collected and stored by or for government and at the same time tightening of the standards under which that information can be inspected, analyzed, and used. We should grant the government necessary authority to access and collect data. The government cannot effectively disrupt criminal enterprises or foil terrorist plots without following a digital data trail that may only appear significant with the passage of time. The trail goes cold if the government does not have initial access and collection capability so that the relationships in the data can be analyzed in context. Note, however, that I am not advocating that private companies build vulnerabilities, like decryption backdoors, into their systems to assist the government. The government should use its own resources; this burden remains on the government.

But even as restrictions on access and collection are loosened, restraints on government inspection (human or robot), analysis, dissemination, and use of that data should be tightened to strengthen civil liberties protections against abuse of that data. In the interest of individual autonomy, this balances the need to preserve useful information with the need to control human access--and possible misuse--of that information.

Second, consider the spectrum of active defense when our enterprises or homes are attacked by cyber criminals, terrorists, or adversary nation-states. I suggest that licensing private actors to defend their networks could help the United States stem the flow of intellectual property—the greatest heist in history. But to mitigate the risks of unintended consequences and uncontrolled escalation of conflict, the government must restrict these licenses to specific activities and set clear rules of the road. In particular, no private party should be allowed to retaliate against or invade another network — even if it is the source of a hacking attack — unless under the direction and control of an appropriate law enforcement or judicial authority.

Third, to avoid fragmentation of the internet, and the consequent huge global economic cost, Congress should work with other countries to develop uniform laws governing both the legal process for obtaining data and the substantive laws governing that data. This will require creation of enforceable treaties or international agreements that focus on protecting the rights of the data subject, since the focus of personal autonomy is reasonable control over one's own data. The objective of this developing international law regime should be to avoid inconsistencies that lead to individual national laws that mandate data localization and thereby compromise the global architecture and freedom of movement of internet data.

Fourth, the law must evolve to control the use private parties can make of individual data. In a world in which people inevitably give off digital exhaust and often cannot give meaningful consent to the use of their data by apps or third parties, the law should shift the default to better protect privacy and autonomy. As some European regulators are currently insisting, this means that enterprises seeking to use data for purposes other than improving the particular service engaged by the user — for example, reselling to third party marketers — should be required to obtain that user's affirmative or "opt-in" consent. Even more explicit consent from the data subject should be mandated when a data aggregator or platform seeks to resell or repurpose an individual's data that was obtained from the third parties who initially collected that subject's data without consent. For those aggregators or platforms whose market position makes them effective monopolists, consent may be deemed insufficient; regulators may need to impose limits on the data uses a monopolist may engage in and might even require a fee be paid by the company to the subject for certain uses.

Most important, the law must limit the ability of corporations to coerce individuals into consenting to broad surrender of control over their data. Thus, the ability of employers or insurance providers to insist on virtually limitless access to individual data as a condition of employment or affordable premiums should be tailored to apply only to information reasonably related to employment or insurability. And data collected for these reasons should be barred from resale or use for unrelated purposes.

Indeed, noting that NGOs have developed transparency indices for how well tech companies respond to government requests for their users' data, we should develop transparent accounts or regulations for how private companies are using, and especially sharing, individual users' data.

Fifth, the law must incentivize private parties to collaborate with the government in protecting against shared vulnerabilities. The vast majority of IT infrastructure is in private hands, but the internet makes it interdependent. Without government expertise and even regulation, coupled with private sector ingenuity and commitment, the internet infrastructure will continue to fall prey to its weakest link. As part of this effort, the law should encourage and protect information sharing directly and in real-time among private and public entities on both industry-focused and regional bases.

Conclusion

If there is an overarching lesson to be drawn from the technology revolution, it is that our day to day lives are described and even defined by data. We generate data, it tracks our behavior, preferences, location and even intentions. Data is used to incentive us, deter us, and even coerce us. If others, be they government or private actors, manage our data, they effectively control much of what we do.

The internet was intended as a force to empower individuals, to forge global connectivity, and even to promote freedom. Although some believe that the internet can be a law-free, almost anarchic zone, I believe that the above demonstrates that without thoughtful rules, the internet can be a tool to constrain individual autonomy, to bully, and to manipulate.

One way to look at the sea of data in which we currently swim is as a global public good. Such a public good has value only if there are rules that prohibit overreaching interference and disruption. We must therefore develop rules to prevent powerful institutions and bad actors from using internet data to damage, rather than enhance, our autonomy.