ConsumersUnion®
POLICY & ACTION FROM CONSUMER REPORTS

July 17, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Attn: Fiona Alexander, Associate Administrator, Office of International Affairs
Washington, DC 20230

Re: Docket No. 17062536-7536-01
Request for Comments on International Internet Policy Priorities

Dear Associate Administrator:

Consumers Union (CU), the advocacy division of Consumer Reports,[1] is an expert, independent, nonprofit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. We write to comment on the questions on International Internet Policy Priorities posed by the National Telecommunications and Information Administration (NTIA).

I. <u>The Free Flow of Information and Jurisdiction</u>

A. What are the challenges to the free flow of information online?

With the open internet protections under United States law now recently undermined and thrown into uncertainty with the passage of the "Restoring Internet Freedom"[2] order by a 3-2 vote at the US Federal Communications Commission (FCC) in December 2017, internet service providers (ISPs) have now gained even greater control over what information their customers see and have access to. ISPs now have the ability to block apps and content or throttle a user's broadband internet service. And they can discriminate between different forms and sources of data flowing

[1] Consumer Reports is the world's largest independent product-testing organization. It conducts its policy and mobilization work in the areas of telecommunications reform, as well as financial services reform, food and product safety, health care reform, and other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million member and publishes its magazine, website, and other publications.

[2] *FCC Releases Restoring Internet Freedom Order*, Fed. Commc'n Comm'n (Jan. 4, 2018), *available at* https://www.fcc.gov/document/fcc-releases-restoring-internet-freedom-order.

through their networks.[3] All of these practices limit the free flow of information online. Complicating this issue is the fact if an ISP choses to block an app or a class of content or platform, this change is not transparent to the end user.

Consumers need the protections that the Open Internet Order provided, and without these consumer safeguards ISPs will be free to repeat the net neutrality violations they perpetuated before 2015. For instance, in 2004, the Madison River Communications company blocked all use of voice over internet protocol services in order to decrease competition with their landline phone service.[4] In 2007, Verizon blocked text messages from the pro-choice group NARAL to their supporters.[5] In 2012 and 2013, AT&T blocked the use of the Apple FaceTime video application on their customer's iPhones. Additionally, in the late 2000s, Comcast blocked BitTorrent traffic on their network.[6] This block also extended to legitimate copyright holders who were sharing their content using this peer-to-peer network.[7]

Importantly, consumers cannot rely on the antitrust laws to provide the needed protections, as some have suggested. The antitrust laws reach only joint conspiracies to restrain trade, efforts to completely monopolize, and mergers. The US Supreme Court's recent decision in Ohio v. American Express Co.[8] is further demonstration of the limits of antitrust.

B. Which foreign laws and policies restrict the free flow of information online? What is the impact on U.S. companies and users in general?

C. Have courts in other countries issued Internet-related judgments that apply national laws to the global Internet? What have been the practical effects on U.S. companies of such judgements? What have the effects been on users?

D. What are the challenges to freedom of expression online?

ISPs and other online actors like platform providers, app developers, and operating systems must be careful to strike a reasonable balance between protecting free expression and protecting users from abuse or harassment. As stated in our response above to I. A., due to the recent repeal of the Open Internet Order by the FCC, ISPs have the ability to restrict access to content online, thus

[3] Matt Stoller, *A Chinese-Style Digital Dystopia Isn't as Far Away as We Think*, BUZZFEED (June 27, 2018), https://www.buzzfeed.com/amphtml/mattstoller2/as-democracy-suffers-digital-dictators-are-seizing-power.

[4] Matt Evans, *How a Triad Company Helped Open the Debate Over Net Neutrality*, TRIAD BUS. J. (May 15, 2014), https://www.bizjournals.com/triad/blog/2014/05/how-a-triad-company-helped-open-the-debate-over.html.

[5] Adam Liptak, *Verizon Reverses Itself on Abortion Messages*, N.Y. TIMES (Sept. 27, 2007), https://www.nytimes.com/2007/09/27/business/27cnd-verizon.html?_r=0.

[6] Declan McCullagh, *Comcast Really Does Block BitTorrent Content After All*, CNET (Oct. 19, 2007), https://www.cnet.com/news/comcast-really-does-block-bittorrent-traffic-after-all/.

[7] *Id.*

[8] *Ohio v. American Express Co.*, SCOTUSBLOG (June 25, 2018), http://www.scotusblog.com/case-files/cases/ohio-v-american-express-co/.

infringing on individuals' freedom of expression. However, other online actors have the ability to discriminate with regards to the information or views users are permitted to express online. Platforms, operating systems, and app developers also pose obstacles to free expression online as a result of their editorial and content control policies.

E. What should be the role of all stakeholders globally—governments, companies, technical experts, civil society and end users—in ensuring free expression online?

As noted above, the repeal of the Open Internet Order has undermined freedom of expression online and we continue to urge reversal of that repeal or, alternatively, voluntary compliance by ISPs with its principles and standards. In addition, both platforms and app developers must do more to ensure that users can exercise their right to free expression.

Our Digital Standard,[9] which is designed to evaluate products for privacy, security, and governance concerns, includes criteria that speaks to the importance of freedom of expression online. One criterion is that the company or organization "publicly commits to respect users' human rights to freedom of expression…"[10] In addition, the Standard states that "the company or organization should have mechanisms in place to implement its commitments to freedom of expression...internally."[11]

For platform providers, creating an acceptable editorial policy, consistent with free expression values but promoting constructive discourse, is an inherently difficult balance. However, while large platforms have a role to play, we cannot entirely rely upon private companies to be the arbiters of societal free expression. Companies should deploy more resources to police platforms for clearly bad behavior but must be careful not to quash divergent viewpoints.[12]

F. What role can NTIA play in helping to reduce restrictions on the free flow of information over the Internet and ensuring free expression online?

The NTIA should encourage companies—including ISPs—to not restrict consumer access to

[9] The Digital Testing Standard (theDigitalStandard.org) was launched on March 6th, 2017 and is the result of a collaboration with our cybersecurity partners, Disconnect, Ranking Digital Rights, and the Cyber Independent Testing Lab. The Standard is designed to hold companies accountable and equip Consumer Reports and other organizations to test and rate products for how responsibly they handle our private data. This is a collaborative and open source effort. The Standard is designed to empower consumers to make informed choices about the connected products, apps, and services consumers use every day. *The Standard*, THE DIGITAL STANDARD, https://www.thedigitalstandard.org/the-standard.

[10] *Id.*

[11] *Id.*

[12] Our Digital Standard supports these ideals, stating: "The company or organization publicly commits to respect users' human rights to freedom of expression and privacy"; "The company or organization should have mechanisms in place to implement its commitments to freedom of expression and privacy internally"; and, "The company or organization should have grievance and remedy mechanisms to address user's freedom of expression and privacy concerns." *Id.*

content online. Although such a self-enforced commitment would not be a sufficient substitution of the protections consumers were entitled to under the Open Internet Order, we encourage the NTIA to pressure ISPs, and other companies, to pledge to protect consumer's access to information and content online.

G. In which international organizations or venues might NTIA most effectively advocate for the free flow of information and freedom of expression? What specific actions should NTIA and the U.S. Government take?

H. How might NTIA better assist with jurisdictional challenges on the Internet?

II. Multistakeholder Approach to Internet Governance

A. Does the multistakeholder approach continue to support an environment for the Internet to grow and thrive? If so, why? If not, why not?

B. Are there public policy areas in which the multistakeholder approach works best? If yes, what are those areas and why? Are there areas in which the multistakeholder approach does not work effectively? If there are, what are those areas and why?

C. Are the existing accountability structures within multistakeholder Internet governance sufficient? If not, why not? What improvements can be made?

D. Should the IANA Stewardship Transition be unwound? If yes, why and how? If not, why not?

E. What should be NTIA's priorities within ICANN and the GAC?

F. Are there any other DNS related activities NTIA should pursue? If yes, please describe.

G. Are there barriers to engagement at the IGF? If so, how can we lower these barriers?

H. Are there improvements that can be made to the IGF's structure, organization, planning processes, or intercessional work programs? If so, what are they?

I. What, if any, action can NTIA take to help raise awareness about the IGF and foster stakeholder engagement?

J. What role should multilateral organizations play in Internet governance?

III. Privacy and Security

A. In what ways are cybersecurity threats harming international commerce? In what ways are the responses to those threats harming international commerce?

Insufficient cybersecurity creates the opportunity for the functionality of large internet-connected systems and the security of information to be compromised. For example, the use of botnets to perpetuate distributed denial of service attacks places large systems at risk and has the potential to bring down large sections of the internet. However, large systems can also be incapacitated through targeted attacks using ransomware. By contrast, data breaches put consumers and their personal information, along with their financial security, at risk. However, both problems could be alleviated if companies were sufficiently incentivized to prioritize cybersecurity. These issues impact international commence by freezing online commerce during an attack and by discouraging consumers from adopting new internet-of-things (IoT) products.

Botnets and DDoS attacks. Botnets have threatened our digital ecosystem since the early 2000s, but the proliferation of connected devices has made it easier for botnets to launch automated distributed denial of service attacks.

A distributed denial of service attack (DDoS) attack is implemented by overwhelming a target server with malicious requests from many internet protocol (IP) addresses. The traffic is created and sent to the target using a botnet (a network of computers infected with malicious software that function as a group without the users' knowledge) that scans the internet for devices that have static or factory default username and password credentials. Once a vulnerable device is detected, the botnet takes control of the device and uses its internet connectivity to overload the target servers with malicious requests that the target is unable to distinguish from legitimate internet traffic. Because a botnet uses multiple vulnerable devices to overload servers with malicious web traffic, the target is unable to stop the attack by blocking a single IP address because there are so many points of origin for the overwhelming amount of internet traffic.

The presence and proliferation of connected devices for consumers, industrial operations, and public infrastructure without sufficient digital security measures endangers the internet that these devices depend on. These concerns require the sustained attention of a variety of experts in and out of the government. Until and unless all connected devices are made more secure, botnet attacks will continue to be a threat. As shown by the October 2016 DDoS attack, botnets have the capability to make large sections of the internet unavailable to users, such as popular sites like Twitter, Reddit, and Paypal. The Mirai virus, the perpetrator of the October 2016 DDoS attack, took down a major infrastructure provider for the internet, Dyn, through an overwhelming amount of fake clicks,[13] also known as click fraud. Click fraud can be used for financial gain since sites like Google pay site owners according to how many clicks they receive on any one advertisement. The continued existence of click fraud through botnets also has the ability to undermine the current economic model of the internet since it is challenging for sites to determine which clicks are legitimate and which are from a botnet and not an individual user. Additionally, botnets can be used to evade spam filters, speed up guessing passwords in order to break into online accounts, and mine bitcoins. The ability to evade spam filters and break passwords more quickly puts consumer data, including highly personal data, at risk. The use of botnets to mine bitcoins also increases the financial incentive for malicious actors to make use of insecure devices.

Due to the continued and increased proliferation of internet-connected devices, as well as the poor security provided on many of these devices, DDoS attacks perpetrated by botnets is expected to increase and continue. Not only are most of the available connected products and services used by consumers,[14] but the danger presented by botnet attacks is only growing as we connect more and more devices that affect our physical security, including medical devices, smart home systems, drones, cars, and other essential devices, to the internet without sufficient security.

Although consumers desire connected devices that can make their lives easier, more efficient, and more productive, consumers are generally unaware or unable to protect against the security concerns posed by vulnerable or outdated IoT devices and accompanying software. Currently, the safety of connected devices is often obscured or unknown to the common consumer. Although earlier forms of attacks on computers, like viruses and worms, affected the functionality of the infected device, newer cybersecurity threats, like the Mirai virus, are difficult or even impossible to detect by a user because they frequently do not affect how users experience the device. Because of this, many owners are unaware that their connected routers, cameras, or DVRs are compromised and part of a botnet attack. In addition, the concern around the security of these connected products has deterred consumers from greater adoption of IoT devices.[15]

Because the poor security of connected devices tends to affect people other than the users or creators of the devices, manufacturers and owners of insecure devices tend to have little incentive to make the devices more secure. Manufacturers are incentivized by the function and features of the device rather than security of the connect product. Many connected products are

[13] There are various ways to commit click fraud. One easy way is to embed a Google ad in a web page that the individual owns. The attacker then instructs all the connected devices on his botnet to repeatedly visit the site and click on the advertisement. Bruce Schneier, *Botnets*, SCHNEIER ON SECURITY (Mar. 1, 2017), https://www.schneier.com/blog/archives/2017/03/botnets.html.

[14] *Gartner Says 8.4 Billion Connected "Things" Will be in Use in 2017, Up 31 Percent from 2016*, GARTNER (Feb. 7, 2017), http://www.gartner.com/newsroom/id/3598917.

[15] Sooraj Shah, *Large-Scale IoT Security Breach Coming in 2017, Forrester Predicts*, INTERNET OF BUS. (Nov. 3, 2016), https://internetofbusiness.com/iot-security-breach-2017-forrester/

shipped with default passwords that are rarely changed by the end user and many connected products are not designed to be patched, rendering the product vulnerable to attack.[16] As a result, government action to increase the security of connected devices—in the form of law enforcement, education, and fostering strong self-regulatory measures—is warranted. Among other things, manufacturers of connected devices should be encouraged to run secure software. This means that IoT devices should be designed with the security of the devices in mind. In addition, products should be regularly patched and updated in order to respond to attacks and prevent vulnerable devices from being hijacked by botnets. Even inexpensive connected devices should be patched regularly and designed with security in mind. Nongovernmental standards—like the Digital Testing Standard[17] that Consumer Reports recently developed and announced with its partners—can play a significant role in strengthening and complementing government efforts to promote stronger security.

We, therefore, urge the NTIA to facilitate increased manufacturer cybersecurity standards for connected products in order to protect our digital infrastructure and the security of consumers and their data.

Ransomware. Large systems can also be compromised by a targeted attack through the use of ransomware, a type of malware that prevents users from accessing their system or computer until a ransom is paid. In May of 2017, WannaCry, a type of ransomware, infected more than 230,000 computers by exploiting a vulnerability in Windows.[18] This gigantic attack affected companies like FedEx, Renault, Deutsche Bahn, and Britain's National Health Service.[19] The WannaCry incident raised awareness of the threat ransomware poses and the importance of timely software patches to fix known vulnerabilities since the threat of the WannaCry ransomware could have been neutralized if companies patched their systems when the Windows update was available in April of 2017.[20] Even a year after the release of the patch, many organizations still had not applied it, leaving their systems open to another WannaCry-type attack.[21] Smaller ransomware attacks have also debilitated state agencies,[22] cities,[23] and local medical centers.[24]Ransomware

[16] Bruce Schneier, *Security and the Internet of Things*, SCHNEIER ON SECURITY (Feb. 1, 2017), https://www.schneier.com/blog/archives/2017/02/security_and_th.html.

[17] *The Standard*, THE DIGITAL STANDARD, https://www.thedigitalstandard.org/the-standard.

[18] Danny Palmer, *WannaCry Ransomware Crisis, One Year On: Are We Ready for the Next Global Cyber Attack?*, XDNET (May 11, 2018), https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/.

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] Following a February 2018 attack on Colorado's Department of Transportation, the state spent between $1 million and $1.5 million recovering from the incident. Benjamin Freed, *Colorado Has Spent More Than $1 Million Bailing Out from Ransomware Attack*, STATESCOOP (Apr. 10, 2018), https://statescoop.com/colorado-has-spent-more-than-1-million-bailing-out-from-ransomware-attack.

[23] In March of 2018, the city of Atlanta, Georgia was the target of a ransomware attack that crippled the city's services for days. The City of Atlanta spent almost $5 million just to procure emergency IT services. James Rogers,

attacks are also extremely costly. In 2017, ransomware attacks accounted for about $5 billion in damages.[25] And in 2019, ransomware damages are estimated to exceed around $11.5 billion.[26] However, companies, governments, and organizations can avoid some ransomware threats by practicing good cybersecurity practices such as updating software regularly to ensure vulnerabilities are patched in a timely manner.

Data breaches. When companies fail to sufficiently protect consumer data, consumers and their data are left vulnerable. Massive data breaches have become commonplace, as companies accumulate vast troves of valuable consumer data but frequently fail to put adequate systems in place to protect it. The Target data breach of 2013 compromised the information of an estimated 110 million people, including the payment card information of about 40 million consumers.[27] Hackers obtained the data of about 80 million people in the Anthem data breach of 2015.[28] And last year, criminals took advantage of well-known vulnerabilities in software used by Equifax to access the Social Security numbers of over 145 million people.[29] Targeted companies often have the opportunity to head off a breach but neglect to take action. For example, the software vulnerabilities that made Equifax a ripe target for attackers had been public for months, but Equifax failed to address them before the breach.[30]

The failure to protect personal data causes real harm to consumers. Over 15 million U.S. consumers fell victim to identity theft in 2016, costing them $16 billion.[31] Victims spend precious time and money repairing the damage to their credit and accounts. Medical identity theft, in which thieves use personal information to obtain medical services, exhausts consumers' insurance benefits and leaves them with exorbitant bills. Tax identity theft occurs when thieves

City of Atlanta Hit by Ransomware Attack, FOX NEWS (Mar. 22, 2018), http://www.foxnews.com/tech/2018/03/22/city-atlanta-hit-by-ransomware-attack.html.

[24] The Erie County Medical Center in Buffalo, New York spent round $10 million responding to a ransomware attack in July of 2017. Henry L. Davis, *ECMC Spent Nearly $10 Million Recovering from Massive Cyberattack*, THE BUFFALO NEWS (July 26, 2017), https://buffalonews.com/2017/07/26/cost-ecmc-ransomware-incident-near-10-million/.

[25] Jaikumar Vijayan, *What Does a Ransomware Attack Cost? Beware of the Hidden Expenses*, CSO (Mar 29, 2018), https://www.csoonline.com/article/3276584/ransomware/what-does-a-ransomware-attack-cost-beware-the-hidden-expenses.html.

[26] *Id.*

[27] Rachel Abrams, *Target to Pay $18.5 Million to 47 States in Security Breach Settlement*, N.Y. TIMES (May 23, 2017), https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.

[28] Brendan Pierson, *Anthem to Pay Record $115 Million to Settle U.S. Lawsuits over Data Breach*, REUTERS (Jun. 23, 2017), https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-us-lawsuits-over-data-breach-idUSKBN19E2ML.

[29] *Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation of Cybersecurity Incident*, EQUIFAX.COM (Oct. 2, 2017), https://www.equifaxsecurity2017.com/2017/10/02/equifax-announces-cybersecurity-firm-concluded-forens ic-investigation-cybersecurity-incident/.

[30] Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sep. 14, 2017), https://www.wired.com/story/equifax-breach-no-excuse/.

[31] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, JAVELIN (Feb. 1, 2017), https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new.

use consumers' Social Security numbers to obtain tax refunds. Fraudulent information on credit reports also causes consumers to pay more for a loan or be denied credit. And breaches take a toll on businesses too—in 2017, the average cost of a breach to companies globally was $3.62 million.[32] But despite these clear harms, little has been done at the federal level to ensure that companies protect sensitive consumer data. As a result, hackers continue to target vulnerable companies—year in and year out, and increasingly from overseas.

However, due to a misalignment of incentives, most companies today do not adequately invest in cybersecurity. Many breaches are not detected or publicly disclosed. The likelihood of law enforcement under the current regulatory scheme is low. The potential profits from using consumer data far outweigh any penalties that can be assessed for violations, incentivizing carelessness and misuse. And companies that experience a data breach bear only a portion of the cost—much of that instead is laid on consumers. As such, we need a much stronger data security law in the United States, and we encourage the NTIA to be supportive of such legislation.

B. Which international venues are the most appropriate to address questions of digital privacy? What privacy issues should NTIA prioritize in those international venues?

IV. Emerging Technologies and Trends

A. What emerging technologies and trends should be the focus of international policy discussions? Please provide specific examples.

One emerging trend that should be the focus of international policy discussions is the increased use of algorithms with little or no accountability.

The increased use of algorithms without sufficient accountability or transparency has the potential to exacerbate existing biases and socio-economic disparities among individuals. Algorithms are now used to serve consumers with targeted ads,[33] decide who qualifies for public benefits,[34] calculate credit scores using alternative data,[35] and set car insurance rates,[36] among other uses. Despite the fact that the use of these algorithms has led to poor outcomes, such as

[32] *Cost of Data Breach Study*, IBM (2017), *available at* https://www.ibm.com/security/data-breach/index.html.

[33] Ryan Singel, *Analysis: Google's Ad Targeting Turns Algorithms on You*, WIRED (Mar. 11, 2009), https://www.wired.com/2009/03/google-ad-annou/.

[34] All Things Considered, *'Automating Inequality': Algorithms in Public Services Often Fail the Most Vulnerable*, NAT'L PUBLIC RADIO (Feb. 19, 2018), https://www.npr.org/sections/alltechconsidered/2018/02/19/586387119/automating-inequality-algorithms-in-public-services-often-fail-the-most-vulnerab.

[35] Kaveh Waddell, *How Algorithms Can Bring Down Minorities' Credit Scores,* THE ATLANTIC (Dec. 2, 2016), https://www.theatlantic.com/technology/archive/2016/12/how-algorithms-can-bring-down-minorities-credit-scores/509333/.

[36] Julia Angwin, et al,, *Car Insurance Companies Charge Higher Rates in Some Minority Neighborhoods*, CONSUMER REPORTS (Apr. 21, 2017), https://www.consumerreports.org/consumer-protection/car-insurance-companies-charge-higher-rates-in-some-minority-neighborhoods/.

individuals in minority-majority neighborhoods being charged more for car insurance, algorithms are still being deployed widely, and often without any public scrutiny of the data used to make decisions about individuals' lives. As the White House's 2014 Big Data states: "Details on what types of data are included in these scores and the algorithms used for assigning attributes to an individual are held closely by companies and largely invisible to consumers. That means there is often no meaningful avenue for either identifying harms or holding any entity in the decision-making chain accountable."[37] We encourage the NTIA to support methods of algorithmic accountability and to urge systematic testing of algorithms to account for biases that may be baked into the automated decision-making process.

B. In which international venues should conversations about emerging technology and trends take place? Which international venues are the most effective? Which are the least effective?

C. What are the current best practices for promoting innovation and investment for emerging technologies? Are these best practices universal, or are they dependent upon a country's level of economic development? How should NTIA promote these best practices?

With the increasing enactment of numerous privacy standards around the globe—including the General Data Protection Regulation in the European Union and the California Consumer Privacy Act here in the US, it is clear that the US needs consistent and comprehensive baseline privacy protections for consumers. Consumers deserve the right to make easy and informed decisions about the collection, use, and retention of their data.[38] In addition, companies that collect and maintain personal information should put in place basic protections that ensure that attackers cannot access it.[39] Consumers should be able to know what data companies maintain about them. Access rights are a fundamental part of privacy laws in Europe and elsewhere and should be in the US as well. US consumers also need a strong enforcement agency to ensure accountability.[40]

In the absence of such a law, CU is doing its part to promote these principles and priorities. As noted above, CU has developed with its partners the Digital Standard,[41] an open standard for testing products for privacy and security in order to help consumers make informed decisions in the marketplace.[42] For instance, one of the important criteria under our Digital Standard[43] is that

[37] *Big Data: Seizing Opportunities, Preserving Values*, EXEC. OFFICE OF THE PRES. (May 2014), p. 46, *available at* https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[38] Consumers Union, *Where We Stand: Congress Should Pass a Strong Privacy Law, Now*, CONSUMER REPORTS (Apr. 9, 2018), https://www.consumerreports.org/privacy/its-time-for-congress-to-pass-a-strong-privacy-law/.

[39] *Id*.

[40] *Id*.

[41] *The Standard*, THE DIGITAL STANDARD, https://www.thedigitalstandard.org/the-standard.

[42] We have published our first set of test results under the Standard and will be releasing more test results in the near future: *Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds*, CONSUMER REPORTS (Feb. 7, 2018), https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/.

the user can see and control everything the company knows about the individual. In order for a company's data practices to be responsible under the Standard, the company must enable the consumer to be able to know to know what user information the company is collecting, the company only requests and collects information that is needed to make the product or service work correctly, and the company explicitly discloses every way in which it uses the individual's data.[44] In addition, the Standard also has criteria relating to how long companies keep consumer data and whether the use knows how long their data is retained.[45]

Thank you for the opportunity to respond to your request for comment on international internet policy priorities.

Sincerely,

Katie McInnis
Policy Counsel

Consumers Union
Suite 500
1101 17th Street, NW
Washington, DC 20036

[43] *Id*.
[44] *Id*.
[45] *Id*.