NetChoice Promoting Convenience, Choice, and Commerce on the Net
Steve DelBianco, President
Carl Szabo, Vice President and General Counsel
NetChoice
1401 K St NW, Suite 502
Washington, DC 20005
www.netchoice.org



July 17, 2018

Fiona Alexander National Telecommunications and Information Administration U.S. Department of Commerce 1401 Constitution Avenue NW, Room 4725 Washington, DC 20230

Subject: International Internet Policy Priorities [Docket No. 180124068-8068-01]

NetChoice offers this response to the National Telecommunications and Information Administration (NTIA) request for comments on the International Internet Policy Priorities [Docket No. 180124068-8068-01].

NetChoice is a trade association of leading e-commerce and online companies, plus thousands of small businesses that rely on e-commerce. We work to promote the integrity and availability of the global Internet and are significantly engaged in Internet issues in the states, in Washington, and in international Internet governance organizations such as ICANN and the IGF.

These comments represent the views of NetChoice and do not necessarily represent the view of any single member or of all members of the trade association.

Below are NetChoice responses to selected requests for comment by NTIA.

#### I. The Free Flow of Information and Jurisdiction

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

#### **Data localization laws**

American Internet startups often race to build an international user base for their platforms, applications, and services. This is an essential strategy for business models building peer-to-peer networks and acquiring large audiences for purposes of advertising.

But it becomes prohibitively expensive for small businesses to acquire users in foreign markets where data localization laws have taken hold. These laws are sometimes explained as ways to protect citizens' privacy and security, but one effect is to prohibit foreign Internet businesses from competing with domestic businesses. It is not financially feasible for startups to acquire technical and legal resources and employ people located in multiple foreign markets.

## **Data privacy laws**

As seen with Europe's *Right to be Forgotten* and General Data Protection Regulation (GDPR), foreign nations are exporting their privacy laws and policies onto US businesses. The General Data Protection Regulation (GDPR) is the most glaring example of this effect, where substantial fines threaten any American business that processes information for a European resident – even if they are on US soil.

The perceived initial success of the GDPR around the globe is encouraging additional governments to create their own GDPR-like regulations. Nations such as Brazil, Vietnam, India, and China have published draft regulations, and some have already become law. This trend is likely to continue.

Europe's *Right to be Forgotten* is a dual threat to American interests. First, US Internet search providers can be sanctioned for failing to suppress search results if a European resident contends that certain content linked to their name should not be revealed in the US.

Second, American Internet users could be harmed if they relied upon search results where relevant results were compelled to be suppressed. For example, US employers, customers, lenders, and vendors could make decisions and enter business transactions because they relied on search results where adverse history of a European subject was deliberately suppressed.

# Tax liability in nations where an American business has no physical presence

European regulators have recently proposed a digital services tax on advertising revenue earned when websites show ads to European eyes. The proposal is a tax of 3% on ad revenue derived from European audiences – whether or not the website has a physical presence in Europe. About half of the impact of this tax would hit US websites viewed by European users.

Again, this tax could hit American businesses that have no physical presence in the European nations levying the tax. This would undermine a fundamental principle of multinational taxation and open the door to additional taxes and regulations across national borders.

# Restrictions on free expression

Governments around the world are enacting laws that restrict free-speech, even leading to arrest of employees of American companies operating in foreign jurisdictions. Turkey, Iran, and Russia have sought to prevent dissident speech, and are holding online platforms liable for content posted by others.

For example, Turkey sought legislation to make it illegal to criticize the country's government.<sup>1</sup> Germany enacted a law that holds platforms liable for hate speech posted by others.<sup>2</sup> The result is that platforms began large-scale purges of *potentially* illegal speech.<sup>3</sup>

We have seen American companies' employees imprisoned when businesses don't comply with foreign mandates to disclose information. Facebook and Google employees, for example, have been arrested in Brazil and Italy for not disclosing the content of stored communications.<sup>4</sup>

<sup>&</sup>lt;sup>1</sup> Carlotta Gall, Erdogan's Next Target as He Restricts Turkey's Democracy: The Internet, N.Y. Times (Mar. 4, 2018).

<sup>&</sup>lt;sup>2</sup> German Network Enforcement Act.

<sup>&</sup>lt;sup>3</sup> Bernhard Rohleder, *Germany set out to delete hate speech online. Instead, it made things worse*, Wash. Post (Feb. 20, 2018)

<sup>&</sup>lt;sup>4</sup> David Meyer, *Brazil Arrests Senior Facebook Exec Over WhatsApp Aid in Drug Case*, Fortune (Mar. 1, 2016), Kashmir Hill, *The Downside of Being a Google Executive*, Forbes (Sept. 27, 2012).

These restrictions will only increase the fragmentation of the Internet and raise costs of entry and legal risks for American businesses with a global online user base.

# Foreign laws and courts that hold platforms liable for content and conduct of users

The first-amendment<sup>5</sup> and free expression are core to our country's values. One way to further these values is for NTIA to encourage other nations to add protections into their laws and trade agreements. To do that effectively, it would be helpful to understand the critical importance and evolution of Section 230 of the Communications Decency Act – the most important Internet law on the books.<sup>6</sup>

Note: The following discussion of Section 230 may seem too detailed for comments to an administrative agency such as NTIA, but we believe the evolution of successful platform liability law in the US is instructive when encouraging other national governments to adopt similar rules. The bottom line is that "Internet 2.0" was all about user-generated content, and American platforms created and dominate this space across the world – thanks to the policy of Section 230.

# Evolution and purpose of Section 230 of the Communications Decency Act

Section 230 was signed into law more than 20 years ago. When the law was conceptualized by Reps. Chris Cox (R-CA) and Ron Wyden (D-OR) in 1995, only 20 million Americans had access to the Internet.

Those who took advantage of this opportunity, including many in Congress, quickly confronted this essential aspect of online activity: many users converge through one portal. The difference between newspapers and magazines versus the World Wide Web was striking. In the print world, humans reviewed and edited content. On the Web, users created content which became accessible to others immediately. While the volume of users was only in the millions, not the billions as it is today, it was evident that no group of humans could keep pace with the growth of content on the Web.

At the time, however, not all in Congress were users of the Web. The Communications Decency Act ("CDA") was premised on the assumption that the FBI could filter the web, screening out offensive content. This was a faulty premise based on a fundamental misunderstanding of the scale and the functioning of the Internet. Nonetheless, in large part because the stated target of the CDA was pornography, the Senate voted overwhelmingly in favor of it.<sup>8</sup>

Section 230 was not part of the original Senate bill. Instead, it was introduced as the Internet Freedom and Family Empowerment Act in the House, which was intended as an alternative to the CDA. As is so often the case in legislative battles between House and Senate, the conferees on the Telecommunications Act of 1996, which became the vehicle for this subject matter, agreed to include both of these diametrically opposed bills. Subsequently, the U.S. Supreme Court gutted the CDA's

3

<sup>&</sup>lt;sup>5</sup> U.S. Const. am. 1.

<sup>&</sup>lt;sup>6</sup> This discussion of Section 230 is drawn from Hon. Chris Cox, *Testimony Before US House of Rep. Energy & Commerce Subcommittee on Communications and Technology Hearing on Latest Developments in Combating Online Sex Trafficking*, (Nov. 20, 2017) on behalf of NetChoice, to House Energy & Commerce Committee, Subcommittee on Communications and Technology, at <a href="https://netchoice.org/wp-content/uploads/2017-11-30-Submission-from-Chris-Cox-on-behalf-of-NetChoice-to-House-Subcommittee-on-Communications-and-Technology-1.pdf">https://netchoice-to-House-Subcommittee-on-Communications-and-Technology-1.pdf</a>

<sup>&</sup>lt;sup>7</sup> 104 P.L. 104, 110 Stat. 56

<sup>&</sup>lt;sup>8</sup> Id.

indecency provisions, as violative of the First Amendment, giving Reps. Cox and Wyden and Section 230 an ultimate victory.<sup>9</sup>

From the point of view of Section 230's authors, the fundamental flaw of the CDA was its misunderstanding of the Internet as a medium. It was simply impracticable, they realized, for bulletin boards, chat rooms, forums, and email that were then budding on the Web to be screened in any meaningful way by the operators of the websites and by fledgling ISPs such as CompuServe and Prodigy. Worse, if the law were to demand such screening, a fundamental benefit of the new medium – facilitating the free exchange of information among millions of users – would be lost.

# The Prodigy and CompuServe cases

Rep. Cox was on a flight to Washington in 1995 when he read a *Wall Street Journal* story about a New York Superior Court case<sup>10</sup> that troubled him deeply. The case involved a bulletin board post on the Prodigy web service by an unknown user. The post said disparaging things about an investment bank. The bank sued for libel but could not locate the individual who wrote the post. So instead, the bank sought damages from Prodigy, the site that hosted the bulletin board.<sup>11</sup>

Up until then, courts had not permitted such claims for third-party liability. In 1991, a federal district court in New York had held that CompuServe was not liable in circumstances like the Prodigy case. The court reasoned that CompuServe "had no opportunity to review the contents of the publication at issue before it was uploaded into CompuServe's computer banks" and therefore was not subject to publisher liability for the third-party content.<sup>12</sup>

But the 1995 New York Superior Court case distinguished CompuServe from Prodigy, because Prodigy sought to impose general rules of civility on its message boards and forums. While Prodigy had even more users than CompuServe and thus even less ability to screen material, the fact it announced such rules and occasionally enforced them was the judge's basis for subjecting Prodigy to liability that CompuServe didn't face.

The perverse incentive this case established was clear: any provider of interactive computer services should avoid even modest efforts to police its site. If the holding of the case didn't make this clear, the damage award did: Prodigy was held liable for \$200 million.<sup>13</sup>

By the time he landed in Washington, Rep. Cox had roughed out an outline for a bill to overturn the holding in the Prodigy case.

# The goals behind creating Section 230

Rep. Cox turned to Rep. Ron Wyden (D-OR) as a legislative partner on his proposed bill. For nearly a year, the Congressmen did outreach and education on the challenging issues involved. In the process, they built not only overwhelming support, but a much deeper understanding of the unique aspects of the Internet that require clear legal rules for it to function.

<sup>&</sup>lt;sup>9</sup> Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).

<sup>&</sup>lt;sup>10</sup> Milo Geyelin, New York judge rules Prodigy responsible for on-line content, Wall St. Jo., May 26, 1995.

<sup>&</sup>lt;sup>11</sup> Stratton Oakmont v. Prodigy Servs Co., 1995 WL 323710 (N.Y.Sup.Ct. May 24, 1995)

<sup>&</sup>lt;sup>12</sup> Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 140 (S.D.N.Y. 1991) (emphasis added)

<sup>&</sup>lt;sup>13</sup> Stratton Oakmont v. Prodigy Servs Co., 1995 WL 323710 (N.Y.Sup.Ct. May 24, 1995)

The rule established in their bill, which they called the Internet Freedom and Family Empowerment Act, <sup>14</sup> was pellucid: the government would impose liability on criminals and tortfeasors for wrongful conduct. It would not shift that liability to third parties, because to do so would directly interfere with the essential functioning of the Internet.

The Congressmen were well aware that whether a person is involved in criminal or tortious conduct is in every case a question of facts. Simply because one operates a website, for example, does not mean that he or she cannot be involved in lawbreaking. To the contrary, as the last two decades of experience have amply illustrated, the Internet – like all other means of telecommunication and transportation – can be used to facilitate illegal activity.

Section 230 was written with a clear and fact-based test:

- If one is a content creator, then one is liable for any illegality associated with that content.
- If one is not the content creator, then one is not so liable.

And what of the case where someone is just partly involved in creating the content? What if, moreover, they were only indirectly involved? In that case, Section 230 comes down hard on the side of law enforcement. In such cases, a website operator who is involved only in part, and only indirectly, is nonetheless deemed just as guilty as the content creator.

Here is the precise language of section 230 in this respect:

The term "information content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet

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

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?

As explained in D above, NTIA can work to encourage trading partners to adopt platform liability protections similar to Section 230. The pitch is not to ask foreign governments to help American Internet companies, but to enable foreign businesses to emulate the success enjoyed by Internet businesses that grew up under America's Section 230 rule.

As explained above, NTIA should educate trading partners about the *domestic downside* of data localization laws. First, the barriers to competition by smaller foreign entrants means that domestic users will have fewer choices among online services. Second, the use of data localization laws cuts both ways. If and when the US and other large markets enact their own policies to require local servers and staff, their home-grown online businesses will find it expensive and legally complicated to serve US and foreign users.

5

<sup>&</sup>lt;sup>14</sup> Internet Freedom and Family Empowerment Act, H.R. 1978, 104 Cong. (1995)

#### II. Multistakeholder Approach to Internet Governance

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

NetChoice is deeply engaged at ICANN and has played a major role in enhancing the multistakeholder accountability structures there. When NTIA announced its intention to transition the IANA contract in Mar-2014, NetChoice was among the skeptics, saying that "accountability to all" was no accountability at all.

However, NetChoice members saw the IANA transition as an inevitable result of the US government's transition plan when it created ICANN. In fact, over 18 years and three administrations, the US government had exercised only light-touch oversight over ICANN.

And in the post-Snowden environment, it was untenable for the US government to forever maintain its unique and unilateral control of the IANA contract. It was clear that retaining US control of IANA would increased the risk of Internet fragmentation and government overreach.

At NTIA's request, the Internet community created a plan to strengthen ICANN's accountability to the global Internet user community and privatize core Internet functions to keep them free from governmental control. NTIA's requirements for the transition guided the design of new mechanisms to: manage core Internet functions; hold ICANN accountable; and prevent government capture after the transition.

NetChoice president Steve DelBianco became a leader on the ICANN cross-community working group that designed the new mechanisms to hold the ICANN board and organization accountable to the community it was designed to serve. The community's proposal met NTIA requirements. Moreover, it reduced governments' power within ICANN by requiring full-consensus for government advice that could oblige the board only to "try and find a mutually acceptable solution."

The transition made ICANN more accountable to the technologists, businesses, civil society, users, and governments who depend upon the Internet to drive economic growth and social evolution around the world. This was a significant improvement on the accountability structures of ICANN that existed prior to the transition.

All of this to show that NetChoice was deeply engaged in the IANA transition from the outset, when Mr. DelBianco first proposed that the IANA transition must be used as leverage – to force ICANN to accept new accountability measures that it would not otherwise embrace.

We explained these new ICANN accountability mechanisms as an invited witness to six Congressional hearings on the IANA transition, between Apr-2014 and Sep-2016:

2-Apr-2014 before House Energy & Commerce Committee, on *Ensuring the Security, Stability, Resilience, and Freedom of the Global Internet*<sup>15</sup>

13-May-2015 before the House Judiciary Committee, on Stakeholder perspectives on ICANN: The .SUCKS domain and essential steps to guarantee trust and accountability in the Internet's operation.<sup>16</sup>

<sup>&</sup>lt;sup>15</sup> https://netchoice.org/wp-content/uploads/NetChoice-Testimony-House-Commerce-IANA-Transition-Hearing-Mar-2014.pdf

<sup>&</sup>lt;sup>16</sup> https://netchoice.org/wp-content/uploads/NetChoice-Testimony-House-Judiciary-ICANN-Hearing-May-2015-FINAL.pdf

13-May-2015 before the House Energy & Commerce Committee, on *Stakeholder perspectives on the IANA Transition.*<sup>17</sup>

17-Mar-2016 before House Energy & Commerce Committee, on *Privatizing the Internet Assigned Numbers Authority* <sup>18</sup>

24-May-2016 before the Senate Commerce Committee, on Examining the Multistakeholder Plan for Transitioning the Internet Assigned Number Authority<sup>19</sup>

14-Sep-2016 before the Senate Committee on the Judiciary, Subcommittee on Oversight, Agency Action, Federal Rights and Federal Courts, on *Protecting Internet Freedom: Implications of Ending U.S. Oversight of the Internet*<sup>20</sup>

Moreover, NetChoice has stayed engaged after for 2 years after the transition to design further ICANN accountability and transparency mechanisms as part of Work Stream 2.<sup>21</sup>

Since the transition, the ICANN community has not yet needed to invoke these new accountability measures. That is partly because ICANN's board and management are keenly aware that the community has significant new powers: to block a proposed budget; direct court enforcement to remove an individual director or to recall the entire ICANN board; and court enforcement of the result of a community-driven Independent Review Process. These are extraordinary measures that we did not expect would be exercised often.

At this point, NetChoice believes that ICANN's accountability structures are adequate to serve the multiple stakeholders of the Internet's numbering and domain name systems. Moreover, ICANN's new bylaws give the Empowered Community new powers to implement further reforms at any time.

#### D. Should the IANA Stewardship Transition be unwound?

In the preceding response, we described how the IANA Stewardship Transition helped to improve IANA's accountability to its customers, and to significantly enhance ICANN's accountability to its stakeholder community. That is the first reason that the transition should <u>not</u> be unwound.

If the transition were unwound, we can see no likelihood of rescuing the hard-won accountability reforms in ICANN's new bylaws. Those reforms were approved only as a complete package, which required compromises by all sides. Those compromises may be irretrievable, as governments and other factions of the ICANN community would seek to improve upon their previous compromise positions. As a result, we might never regain the strong accountability powers approved as part of the transition.

The second reason the transition should not be unwound is to maintain the security and stability of the internet's unique identifiers. One of the great successes of the stewardship transition has been the

<sup>&</sup>lt;sup>17</sup> https://netchoice.org/wp-content/uploads/NetChoice-Testimony-House-Commerce-ICANN-Hearing-FINAL.pdf

 $<sup>\</sup>frac{18}{\text{https://netchoice.org/wp-content/uploads/NetChoice-Testimony-House-Commerce-ICANN-Hearing-Mar-}}{2016.pdf}$ 

<sup>&</sup>lt;sup>19</sup> https://netchoice.org/library/netchoice-testimony-us-senate-commerce-committee-examining-multistakeholder-plan-transitioning-Internet-assigned-number-authority/

<sup>&</sup>lt;sup>20</sup> https://netchoice.org/library/testimony-u-s-senate-committee-judiciary-subcommittee-oversight-agency-action-federal-rights-federal-courts/

<sup>&</sup>lt;sup>21</sup> See https://community.icann.org/display/WEIA/WS2+-+Enhancing+ICANN+Accountability+Home

continued security and stability of the underlying technology for which we designed the accountability mechanisms described above in item II.C. The ability for a global set of technologists to contribute solutions to the needs of an ever-expanding global set of customers continues to improve the resiliency of this technology through expansion, diversity, and redundancy.

The third reason against any attempt to unwind the transition is that it would re-kindle the fire at the United Nations, who saw the legacy US government role as something the UN should have been doing instead.

One motivation for the transition was to eliminate the role where one government alone (the US) held ICANN accountable, and instead make ICANN accountable to the community of Internet stakeholders. Once we completed the transition, the UN and ITU could no longer point to the US government role and insist that the UN should step into those shoes.

But if the US attempted to unwind the transition, it creates the perfect excuse for the United Nations and a growing number of US critics to do what they have long sought: to move ICANN and IANA functions into the UN system and relocate these functions outside the US. This would reduce US ability to influence ICANN policies and hold it accountable to American interests.

In 2011, a group of governments proposed their own UN replacement for US oversight and ICANN's model of private sector leadership. India, Brazil, and South Africa declared it was time for "establishing a new global body" located "within the UN system" to "oversee the bodies responsible for technical and operational functioning of the Internet."

US industry is actively working to defeat proposals by some governments that would have the ITU regulate everything from cloud services and the Internet of Things to digital payments. These regulations would be a significant impediment to innovation by many American companies. The successful IANA transition showed that governments and intergovernmental organizations are ill-suited to deal with complex issues within ICANN, where bottom-up processes work best. To even talk about unwinding the transition will send the opposite message.

The governments of China and Russia would exploit any talk of unwinding the transition to persuade moderate governments that the UN needs to replace the legacy US government role. Discussions of the US government reclaiming IANA signals to the world that the legacy US role in IANA was so important that it must be recaptured. And that will make the IANA contract role a shiny object that the UN aspires to claim for itself.

Unwinding transition could create far more downside than upside for the interests of US government, businesses, and citizens.

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

NTIA should use its role in ICANN's Government Advisory Committee (GAC) to help government representatives develop specific and timely advice on matters that are relevant to governments. Priority issues include:

- Coordinate GAC outreach to European Data Privacy regulators, in order to preserve access to registrant information that is needed for legitimate purposes such as consumer protection, fraud prevention, and Intellectual property rights.
- Coordinate a process to digest national regulations inspired by the GDPR, to facilitate the efficient development of solutions that preserve access to registrant information as indicated above.

- Seek a compromise resolution to address GAC's original advice against the .AMAZON top-level domain.
- Encourage GAC to develop a coherent and workable position regarding domain names of geographic or cultural significance, to enable the next round of new top-level domains.
- Increase GAC's substantive participation in community-driven reviews such as Accountability & Transparency, and Security, Stability and Resiliency.

## F. Are there any other DNS related activities NTIA should pursue?

Here are three potential areas for NTIA to pursue, relative to the Domain Name System (DNS):

- consider ways to increase DNS Security (DNSSec) deployment globally, and promote domestic deployment of DNSSec to combat DNS hacks by criminals and by America's enemies.
- explore ways to improve the resilience of the root server system so that it will be more resistant to denial-of-service attacks by criminals and by America's enemies.
- consider how to improve universal acceptance of domain names and email addresses that use new top-level domains (gTLDs), particularly those with character sets beyond the Latin alphabet. While ICANN has enabled a significant expansion of top-level domains, registrants in many of those new domains are still unable to enter their website or email addresses on web forms that were coded only for legacy gTLDs. And some email filtering systems have failed to keep up with the many new TLDs being used today, particularly in scripts and languages other than English.
  - 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?
  - I. What action can NTIA take to help raise awareness about the IGF and foster stakeholder engagement?

NetChoice has attended all of the global IGF meetings and spoken on many IGF panels and sessions. While it is certainly true that travel expense is a barrier for individuals and small businesses to attend the annual global IGF event, the costs for remote, real-time participation are extremely low.

In addition, many nations have national/regional IGF organizations whose events would not require international travel. NetChoice was a founding member of the IGF-USA, an event we hold each year to galvanize interest in the global IGF and gather input on issues and priorities of American Internet stakeholders.

NTIA should continue to participate in and support the global IGF and IGF-USA events, both as a way to feed-in the priorities of American commerce, and to report-back on relevant issues and trends.

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

Governments have an enduring sovereign claim to govern what occurs within their borders, whether online or offline. And multilateral organizations of governments, such as the UN and ITU, have a growing interest in asserting the power of governments to control online content and conduct that crosses borders.

Multilateral organizations like the UN and ITU increasingly assert themselves as alternatives to the multistakeholder approach that ICANN employs to coordinate the Internet's naming and numbering systems. For that reason, the US government must avoid unilateral actions or provocative moves that could create a pretense for anti-American governments to say that ICANN and/or IANA are under US control. Critics of the multistakeholder model could exploit US action to convince even moderate governments that a multilateral model was better than a multistakeholder ICANN where the US had unilateral sway.

## **III. Privacy and Security**

We welcome the opportunity to work with NTIA to identify national themes and develop policies and principles that protect privacy while avoiding unintended consequences that could prevent American business innovation.

NetChoice encourages NTIA to continue its prior efforts to meet with US stakeholders seeking policy solutions for privacy and security challenges. NetChoice has been an active participant in previous NTIA multistakeholder processes aimed at digital privacy. While prior efforts have not always resulted in consensus solutions, NetChoice believes NTIA's efforts were highly valuable to frame issues and specifically identify different perspectives among single-focus privacy advocates and broader-focus business stakeholders.

At the same time, NTIA should seek opinions and views from those who are not otherwise vocal, via polling and meetings outside the beltway and away from the coasts. This can help better identify themes of privacy and security that resonate with all Americans.

Such discussions should focus on clarifying terms like: personal information, biometric information, and processing. For example, would a sign being displayed in public constitute personal information? Would a photograph of that publicly displayed sign constitute personal information? Would a photograph constitute biometric information? Would using a ruler on a topographical map constitute processing? Core terms like this lack clarity and create confusion for users and businesses alike.

Outside the US, NTIA should probably not attempt to convene multi-national stakeholders to address global concerns about privacy and security. Rather, NTIA can bring its commerce-focused views to multistakeholder discussions at ICANN and the IGF.

As noted above, NTIA should argue against foreign nations exporting their privacy laws and policies onto US businesses. The General Data Protection Regulation (GDPR) is the most glaring example of this effect, where substantial fines threaten any American business that processes information for a European resident – even if they are on US soil.

Europe's *Right to be Forgotten* is another threat to American interests, in two important ways. First, American Internet search providers can be sanctioned for failing to suppress search results if a European resident contends that certain content linked to their name should not be revealed in the US.

Second, American Internet users could be harmed by relying on search results where material and relevant results are compelled to be hidden. For example, US employers, customers, lenders, and vendors could make decisions and enter business transactions because they relied on search results where adverse history of a European subject was deliberately suppressed.

NTIA should make it a priority to protect American businesses and consumers from costs and burdens imposed by international Internet regulators, lawmakers, and courts.

NetChoice appreciates the opportunity to provide these comments and stands ready to expand further on any topics relevant to NTIA's work on international Internet priorities.

Sincerely,

Steve DelBianco Carl Szabo

President Vice President and General Counsel

NetChoice NetChoice

NetChoice is trade association of leading e-commerce and online businesses. www.NetChoice.org