ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

26 de junho de 2012

Deputado Alessandro Molon
Praça dos Três Poderes — Câmara dos Deputados
Gabinete: 652 - Anexo: IV
70160-900 Brasília, DF
a/c Pedro Paranaguá *(por email)*

Excelentíssimo Senhor Deputado:

Peço suas desculpas (e as de outros leitores brasileiros) por ter escrito em inglês e espero que isso não seja uma dificuldade.

Thank you for the Marco Civil draft with proposed modifications as of June 16, which we received from Pedro Paranaguá. These comments on behalf of the Electronic Frontier Foundation refer to that draft.

About EFF

The Electronic Frontier Foundation (EFF) is a non-profit, member-supported civil liberties organization working to protect rights in the digital world. EFF actively encourages and challenges industry, government and the courts to support free expression, privacy, and openness in the information society. Founded in 1990, EFF is based in San Francisco, California. EFF has members all over the United States and throughout the world.

In general

The adoption of this draft would be a significant victory for the protection of Brazilians' civil liberties on-line in almost all respects. With the exception of article 11, the provisions of the draft Marco Civil are all comparably protective of free expression and user privacy and autonomy to current law in the United States, and in several cases the Marco Civil draft is even more protective of these values. As civil libertarians, we appreciate the numerous ways in which this proposal protects Internet users.

Article 8

We appreciate the entirety of this article, including the explicit statement of respect for users' choices of privacy-enhancing technologies in the article's sole

454 Shotwell Street • San Francisco, CA 94110 USA
v +1 415 436 9333 f +1 415 436 9993 i www.eff.org e information@eff.org

paragraph. We think technology has an important role to play in protecting privacy on-line; we have campaigned for Internet users' access to and understanding of the technologies that help protect privacy and we welcome statements in support of this access in law.

Article 9

Protecting network neutrality is vitally important. But defining what network neutrality should mean in practice, on an operational level, can be a surprisingly complex task. Among the controversies that can arise is what ISPs may do to prevent spam and abuse on their networks—particularly if some users may disagree with an ISP's judgment about what constitutes spam or abuse, or if some users believe that automated anti-abuse systems are too prone to errors and blocking legitimate traffic. Another kind of controversy is whether service providers may include explicitly non-neutral terms in their terms of service and then enforce those terms by technical means (for example, terms prohibiting users from running public servers from residential Internet connections, or from sharing their connections with the general public).

The network neutrality debate in the United States has also expanded over time to include economic arguments about interconnection and peering fees between service providers, and, more broadly, who is responsible for paying for new infrastructure to better interconnect existing providers as traffic increases. Interconnection between telephone carriers in many countries has been regulated by government agencies which established detailed regulatory regimes governing who has to pay what to whom and who has to offer interconnection to whom on what sort of terms. In most places there has not been analogous regulation of Internet service providers' interconnection; instead, it has been negotiated privately. Large providers have usually understood that it was in their mutual interest to interconnect and exchange traffic, in some cases including the payment of settlement fees from one provider to another.

Sometimes, a failure to reach agreement could create infrastructure problems that can be seen as neutrality problems: inadequate capacity and interconnection from one part of the Internet to another means that users trying to reach other users or services on particular remote networks will have slow or unreliable service, even if connectivity elsewhere is fast and reliable. The most famous recent disputes over interconnection terms have involved Level 3 and Cogent (in 2005), Cogent and Telia (in 2008), Sprint and Cogent (in 2008), and Level 3 and Comcast (in 2010); in some of these cases, customers on different parts of the Internet briefly lost connectivity and became unable to reach each other as a result of commercial disputes. There is not a clear consensus that these incidents

should be regarded as neutrality problems at all, and all were eventually resolved by further negotiation.

The surprising level of technical and economic detail that can result from trying to specify what intuitively feels like an extremely simple principle—"treat the various users, applications, and parts of the network alike"—mean that network neutrality regulation needs to tread carefully and ensure that those devising regulations are institutionally up to the task: sophisticated technically and economically, and able to resist capture and undue influence from parties who may pressure them to define "neutrality" in ways that perversely may actually threaten neutrality. Regulation in this area can easily go awry in the course of translating high-level policy goals into concrete technical requirements, and the political pressures on the regulators are likely to be intense.

With regard to the obligation in § 2º for providers "informar aos seus usuários sobre as práticas de gerenciamento de tráfego adotadas", we suggest that the providers should provide relevant technical details for interested users, and not merely high-level summaries or general descriptions of their practices. There is a considerable risk that providers might attempt to comply with their obligations by making general, vague statements. Most importantly, end-users should not be put in a position where it's impossible for them to diagnose the reasons why particular communications are slow or unreliable because they can't get the specific information they need from ISPs. ISPs should always work cooperatively with their users, with other ISPs, and with the broader technical community to ensure that it's clear who or what is at fault for outages and connectivity problems.

With regard to § 4º, we wonder whether it's possible at this stage to put limitations, either substantive or procedural, on the sorts of exceptions to neutrality that are admissible.

It would also be helpful to know more about how the neutrality rules will be enforced and how alleged violations of neutrality will be investigated. For example, will individual end-users have the right to bring court actions against service providers for alleged violations?

Article 11

This article imposes a telecommunications data retention mandate similar to data retention rules in some other countries. We recognize that the mandate contemplated here is somewhat narrower than those proposed or implemented elsewhere—for instance, the limitations on retention in Article 12 provide greater

privacy protection than other data retention laws we've examined. EFF remains opposed to mandatory telecommunications data retention and continues to campaign against it in the United States and in conjunction with partner organizations in other countries. We recommend deleting this article in its entirety.

Although telecommunications data retention mandates have been adopted in some places (particularly in the European Union member states since 2006, pursuant to EU Directive 2006/24/EC on telecommunications data retention), these laws have been extensively criticized by civil society, and in some cases challenged in court. As a result of these challenges, several national constitutional courts have found particular national data retention laws unconstitutional. These include the constitutional courts of Romania (in 2009), Germany (in 2010), the Czech Republic (in 2011), and the Supreme Court of Argentina (in 2009). The European Court of Justice is also considering a challenge to the Directive as a whole on human rights grounds arising from a case in the Irish High Court.

We would like to emphasize that *the United States does not have a telecommunications data retention mandate for Internet service providers*. Unlike the cases just mentioned, this is not a result of a constitutional court decision; rather, the U.S. Congress has never adopted such a mandate. We think it is a disproportionate harm to privacy to require the collection of personal information about members of the general public who are not charged with or suspected of a crime, so we continue to oppose data retention mandates in the United States and elsewhere.

Current U.S. law allows law enforcement and other parties to require service providers to preserve specific information already collected when that information may be relevant to a criminal investigation or court case. In our experience, service providers have complied with this obligation; we haven't seen evidence that the status quo in the U.S. has hindered the investigation of serious crimes.

Article 13

This article regulates how application service providers may store records about users. In most respects this article is more privacy-protective than relevant U.S. law; it's more comparable to the norms in European jurisdictions which follow a data-protection model (particularly §§ 2º, 3º, and 4º). We think § 5º and § 6º, on access to data for judicial processes, are broadly similar to current U.S. legal rules on the same subject, with some technical differences.

We suggest making more explicit the standards or requirements for secure storage (although perhaps this will be a consequence of implementing regulations: "Art. 10 § 2º As medidas […] de segurança e sigilo devem […] atender a padrões definidos em regulamento"). We particularly suggest adding some form of *breach notification* obligation. Breach notification exists as a matter of state law in many states in the United States (including EFF's home state of California), though not yet at the Federal level. A breach notification obligation means a duty of an organization that holds personal data about individuals to notify the subjects of that data when that data has been lost or stolen by a malicious party. This kind of obligation has at least two important benefits: it allows individuals to better understand and take precautions against fraud and impersonation ("identity theft") that might be committed using stolen data about them, and it better aligns the incentives of companies with individuals about whom they retain data, providing a concrete incentive to implement strong controls and take strong precautions against losing control of sensitive personal information.

For California's data breach law, see California S.B. 24 (2011), codified at Cal. Civ. Code §§1798.29, 1798.82.

Articles 14, 15, and 16

We have always emphasized that Internet intermediaries have a major role to play in enabling free speech on-line and that protections for intermediaries are among the most important aspects of Internet policy. We've worked in the U.S. courts to defend the broad protections for intermediaries under U.S. law, because we know that when intermediaries face significant legal uncertainty, they may react by avoiding anything controversial. We applaud the strong protections for Internet intermediaries in this draft.

Article 16 calls for users to be informed when their content has been removed. If the reason for the removal was a court order of which the user was previously unaware, the user might choose to retain a lawyer in order to challenge or appeal that order. Although this is probably already implied by "os motivos e informações relativos à remoção de conteúdo", we think it would be worth saying explicitly that the provider should in this case communicate the name of the court and the specific court case name or number, because the user's lawyer will require this data in order to obtain more information, and in order to challenge or appeal the order. We also think that the user should be informed as promptly as is practical; if a user believes that the removal of content was a mistake, the user will presumably want to start the process of challenging it as soon as possible.

Article 16 §§ 1º and 2º suggest an innovative approach to transparency in cases of content removal. We think this sort of transparency is extremely valuable to users; it provides a contrast to the current situation in China, where the government reportedly encourages providers to disguise content removals and censorship as technical errors, so that users have no way of knowing that they were deliberate, or that anything in particular has been blocked, or why, or by whom. Instead, removed content vanishes as if it had never existed, and the providers involved pretend nothing has happened. The transparency practices suggested by these paragraphs are exactly the opposite of this situation. We appreciate the practice of some hosting providers of clearly distinguishing between materials that have been removed and materials that never existed, as well as of giving as much information as possible about why materials were removed. Doing so is responsible and respectful toward users, seeking to inform them rather than keep them in the dark.

However, it's not clear that this transparency requirement—as a legal duty for application providers and hosts—could be implemented this way in the United States as a matter of free speech law, because of the limitations it places on the editorial judgment of publishers; it may be worth considering this impact as well, since it seems strange to suggest that *every* Internet forum has a duty to the public to publicly account for each content removal decision that it makes. This is of particular concern for Internet application providers who see themselves as editorially involved in the selection of content and who have removed content without being legally compelled to do so.

Thanks for the opportunity to comment on this draft, and please let us know if we can elaborate on anything we've said here.

Atenciosamente,

Seth Schoen
Senior Staff Technologist