



Follow us

@IBAEvents #IBAWashington



IBA2016

**18–23 SEPTEMBER
WASHINGTON DC**

ANNUAL CONFERENCE OF THE INTERNATIONAL BAR ASSOCIATION

OFFICIAL CORPORATE SUPPORTERS





villão 🍷



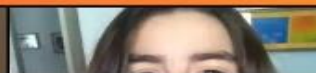
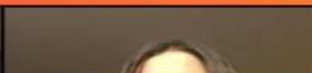
@v_i_l_l_a

brazil, 12 🇧🇷 💕💕

174
seguindo113
fãs4701
curtidas

editar perfil

270 musical.lys, 8660 corações



32



Introduction

“frequently the disruptive innovations bring benefits to the consumers such as convenience, simplicity and lower costs”, but “the changes are not well seen by the solidified companies in the market, that try to maintain their positions by using the current legislation” (Cezar Taurion – manager of new technologies at IBM Brazil)



UBER



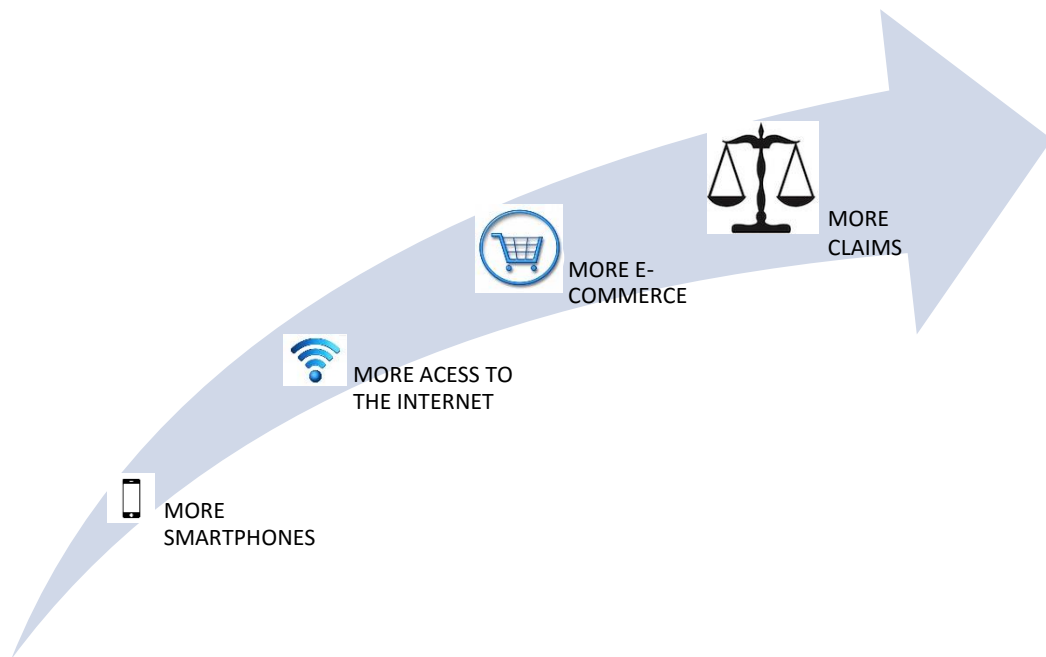
IBA2016 18–23 SEPTEMBER
WASHINGTON DC


ANNUAL CONFERENCE OF THE INTERNATIONAL BAR ASSOCIATION


OFFICIAL CORPORATE SUPPORTERS





Issues regarding the protection of consumers using digital platforms



 The arrival of new technologies and general price drop increased substantially the number of smartphones in Brazil (in 2015, 76.1 million consumers had their own smartphone).

 Consequently, access to the internet also went thru substantial increase, specially in less wealthy social classes.

 This increased the number of Brazilians consuming thru e-commerce (a growth of more than 1000% in the last 10 years).

 As a result, Brazil is experiencing an increase in problems such as complaints of consumers using digital platforms, bringing new challenges mainly about the policy of the companies on return and replacement of products sold online.



IBA2016 18–23 SEPTEMBER
WASHINGTON DC

ANNUAL CONFERENCE OF THE INTERNATIONAL BAR ASSOCIATION

OFFICIAL CORPORATE SUPPORTERS



United States Overview

- No single comprehensive national law that protects all categories of personal data or the collection and use of that data.
- No single authority tasked with overseeing digital data protection.
- Industry or sector related - - Various state and federal laws regulate different categories of personal data.
- At the state level, attorneys general also have the ability to bring enforcement actions for unfair or deceptive trade practices, or to enforce violations of specific state privacy laws. Some state privacy laws allow individuals to bring lawsuits to enforce violations.
- Various state laws generally limit what can be done with the personal data collected and provide notification requirements if personal data is breached.

Data Protection In Regulated Industries

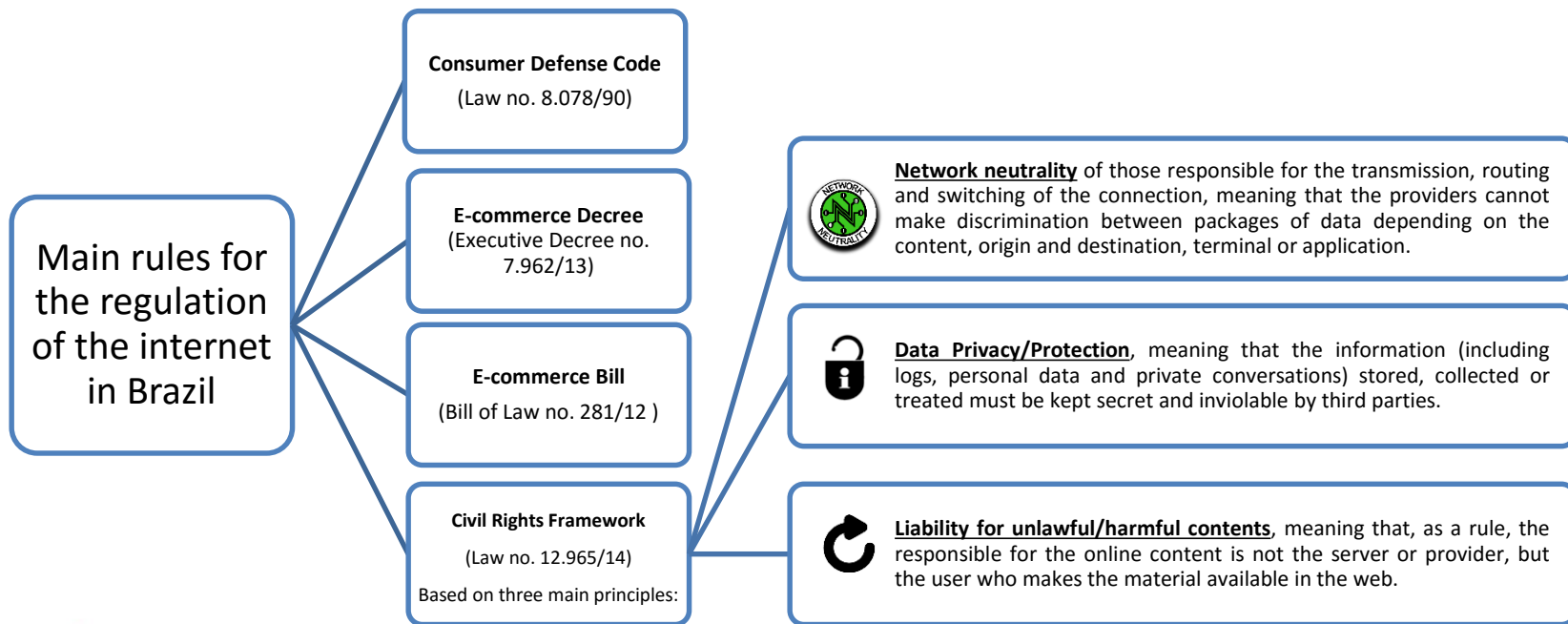
- The Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act) (regulates unfair and deceptive business practices including those related to online privacy and data security).
- Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§6501-6506) (regulates the collection of information from children).
- The Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827) (regulates the collection, use and disclosure of financial information by financial institutions such as banks, securities firms and insurance companies; enforced by Consumer Financial Protection Bureau and various financial services regulators (as well as state insurance regulators)).
- The Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 *et seq.*) - - regulates collection, use, protection and transfer of medical information and applies to health care providers, data processors, pharmacies and other entities that come into contact with medical information; enforced by Department of Health and Human Services.

Other Federal Data Protection Laws

- The Fair Credit Reporting Act (15 U.S.C. §1681) applies to consumer reporting agencies, those who use consumer reports (such as a lender and credit card companies) and regulates the use and disclosure of consumer's creditworthiness, credit history, credit capacity, character, and general reputation.
- The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) (15 U.S.C. §§7701-7713 and 18 U.S.C. §1037) regulates the collection and use of e-mail.
- The Telephone Consumer Protection Act (47 U.S.C. §227 *et seq.*) regulates the collection and use of telephone numbers.
- The Electronic Communications Privacy Act (18 U.S.C. §2510) (regulates the interception of electronic communication).
- Computer Fraud and Abuse Act (18 U.S.C. §1030) (regulates computer tampering).

- FTC – Regulatory Tools

Specific regulation



IBA2016

18–23 SEPTEMBER
WASHINGTON DC

ANNUAL CONFERENCE OF THE INTERNATIONAL BAR ASSOCIATION

OFFICIAL CORPORATE SUPPORTERS



Legal instruments to deal with rights of consumer that use digital platforms and its effectiveness



PROCON (Consumers Protection Agency): 678 units throughout all 27 Brazilian States. the State of São Paulo itself registered in 2015 1,050,352 customer complaints and consultations.



JEC (Small Claims Courts): limited to 40 minimum wages (approximately USD 12,500.00), these courts became a very popular and fast way for the consumers to get justice done. By the end of 2015, Brazil had more than 17 million ongoing lawsuits before JECs.



IBA2016

18–23 SEPTEMBER
WASHINGTON DC

ANNUAL CONFERENCE OF THE INTERNATIONAL BAR ASSOCIATION

OFFICIAL CORPORATE SUPPORTERS



Legal instruments to deal with rights of consumer that use digital platforms and its effectiveness



Public Civil Actions: powerful proceedings, the civil class actions can be filed only by **certain entities** and have as main characteristic the **defense of interests of the collectivity** or diffuse rights.

Private institutions: websites that review and evaluate products and services, as well as intermediating complaints deriving from consumer relationships. Similar to the world-wide-famous Better Business Bureau. As an example, Reclame Aqui has over **120,000 registered and evaluated companies** and over **15,000,000 registered consumers** that access its webpage in order to verify companies' ranks.

ReclameAQUI



Regulatory Agencies: ANATEL is the Brazilian regulatory agency in charge of telecommunications, including landline phones, mobile phones, internet (mobile and cabled) connection and television services.



IBA2016 18–23 SEPTEMBER
WASHINGTON DC

ANNUAL CONFERENCE OF THE INTERNATIONAL BAR ASSOCIATION

OFFICIAL CORPORATE SUPPORTERS



Data Breach Notification

- Almost all states and the District of Columbia have data breach notification statutes.
- These generally require notifying state residents if there is a security breach involving residents' sensitive information (typically name plus another sensitive data element (*e.g.*, social security number, credit card or financial account number)).
- Generally cover entities that conduct business in the state and that own, license or maintain covered information.
- Most cover timing of the notice (*e.g.*, most expedient time possible and without unreasonable delay).
- Some require government notification as well.
- Set forth penalties for failure to provide timely notice.

Data Breach Notification

- California - - Cal. Civ. Code § 1798.82
- Florida - - Fla. Stat. § 501.171
- Mass. - - Mass. Gen. Laws ch. 93H, §§ 1- 6
- New York - - N.Y. Gen. Bus. Law § 899-aa
- Texas - - Tex. Bus. & Com. Code §§ 521.002, 521.053, 521.151
- Virginia - - Va. Code Ann. § 18.2-186.6

State Preventative Laws

- A number of states have also enacted preventative laws to try and avoid a security breach.
- *See, e.g.,* Massachusetts Regulation (201 CMR 17.00).
- Provides for an extensive list of security protocols aimed at protecting personal information that affected companies must implement into their security architecture, and describe in a comprehensive written information security program.

- FTC – Multi-jurisdictional Issues

Enforcement of consumers' right of privacy

Privacy Protection in the Civil Rights Framework for the Internet

Privacy protection must guide the use of the internet (art. 3, II)

Privacy protection is a condition for the perfect exercise of the right to access the internet (art. 8)

All companies that collect, store, keep and treat any kind of data or information must respect the right of privacy, protection of data and confidentiality of private conversations and logs (art. 11)

Right of non-disclosure to third parties of users' personal data, including connection logs and logs of access to internet applications, unless with express, free and informed consent (article 7, VII)



IBA2016 18–23 SEPTEMBER
WASHINGTON DC
ANNUAL CONFERENCE OF THE INTERNATIONAL BAR ASSOCIATION

OFFICIAL CORPORATE SUPPORTERS



Responsibility for privacy violations

Consumer Defense Code

Any company or entity involved in the production chain may be held responsible for defects in the product or service delivered to the final consumer

Civil Rights Framework for the Internet: same logic of the Consumer Defense Code (any operation that take place in Brazil is must obey such Law), mitigated as follows

Internet providers will not be civilly responsible for damages caused by content posted by third parties (art. 18)

If there is no incomppliance of a judicial order, websites are not civilly responsible for the exposure of a given content (art. 19)

In cases of unauthorized publication of intimate images, the content provider (website or webhost) has the obligation to remove the harmful content only once notified by the interested Party (art. 21)



IBA2016 18–23 SEPTEMBER
WASHINGTON DC

ANNUAL CONFERENCE OF THE INTERNATIONAL BAR ASSOCIATION

OFFICIAL CORPORATE SUPPORTERS



- FTC – Consumer Privacy

Criminal vs. Civil Penalties

- Violations of federal and state privacy laws generally lead to civil, not criminal, penalties.
- The main exceptions are the laws directed at surveillance activities and computer crimes.
 - Electronic Communications Privacy Act (ECPA) (which is composed of the Wiretap Act, the Stored Communications Act, and the Pen Register Act).
 - Computer Fraud and Abuse Act (CFAA) can lead to criminal sanctions and civil liability.
 - Certain state surveillance laws.
- US Department of Justice is authorized to criminally prosecute serious HIPAA violations (knowingly obtaining and disclosing health information).

Private Lawsuits

- Plaintiffs in individual and class actions typically claim that the defendant failed to adequately protect plaintiffs' personal information, used that information for unauthorized purposes, e.g., online “tracking” or behavioral advertising, or otherwise violated their privacy rights under state or federal statutes or common law.

Private Lawsuits - Standing

- *See. e.g. Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386 (6th Cir. Sept. 12, 2016).
- Sixth Circuit panel held that plaintiffs had standing to assert claims arising from hackers' alleged theft of data containing plaintiffs' sensitive personal data. Held that hackers' targeted theft of personal identifying information ("PII") created a substantial risk of harm that is sufficient to satisfy the concrete injury requirement for standing under Article III of the United States Constitution.

Electronic Marketing

- The US regulates marketing communications including email and text message marketing.
- CAN-SPAM Act - -
 - federal law that applies labelling and opt-out requirements to all commercial email messages.
 - generally allows a company to send commercial emails to any recipient, provided the recipient has not opted out of receiving such emails from the sender; the email identifies the sender and the sender's contact information.

Administrative Rulemaking Activity

- The Federal Communications Commission announced in April 2016 a notice for proposed rule-making relating to protecting consumers' privacy when using broadband services.

"the current federal privacy regime, including the important leadership of the Federal Trade Commission (FTC) and the Administration efforts to protect consumer privacy, does not now comprehensively apply the traditional principles of privacy protection to these 21st Century telecommunications services provided by broadband networks."

Recent Legislative Activity

- Judicial Redress Act (2016) - -
 - giving citizens of certain ally nations (notably, EU member states) the right to seek redress in US courts for privacy violations when their personal information is shared with law enforcement agencies.
 - authorizes the Department of Justice to designate foreign countries or regional economic integration organizations whose natural citizens may bring civil actions under the Privacy Act of 1974 against certain U.S. government agencies for purposes of accessing, amending, or redressing unlawful disclosures of records transferred from a foreign country to the United States to prevent, investigate, detect, or prosecute criminal offenses.

Legislative Activity

- H.R. 2205 (Data Security Act of 2015), which would require individuals, corporations, or other non-government entities that access, maintain, communicate, or handle sensitive financial account information or non-public personal information to implement an information security program and to notify consumers, federal law enforcement, appropriate administrative agencies, payment card networks, and consumer reporting agencies of certain data breaches of unencrypted sensitive information likely to cause identity theft or fraudulent transactions on consumer financial accounts.
- H.R. 699 (Email Privacy Act) amends the Electronic Communications Privacy Act of 1986 to prohibit cloud computing service provider from knowingly divulging to a governmental entity the contents of any communication (such as email) that is in electronic storage or otherwise maintained by the provider, subject to exceptions (generally requiring warrant) (Passed House unanimously in April 2016).