SQUIRE PATTON BOGGS

Comisión de Regulación de Comunicaciones
REPÚBLICA DE COLOMBIA

IX INTERNATIONAL REGULATORY WORKSHOP: TRENDS AND CHALLENGES IN THE ICT SECTOR

The Internet: Security, Privacy and Confidentiality Issues

Ann LaFrance
Co-Chair, Global Data Privacy and Cybersecurity Group
Squire Patton Boggs (UK) LLP
ann.lafrance@squirepb.com

Agenda

SQUIRE PATTON BOGGS

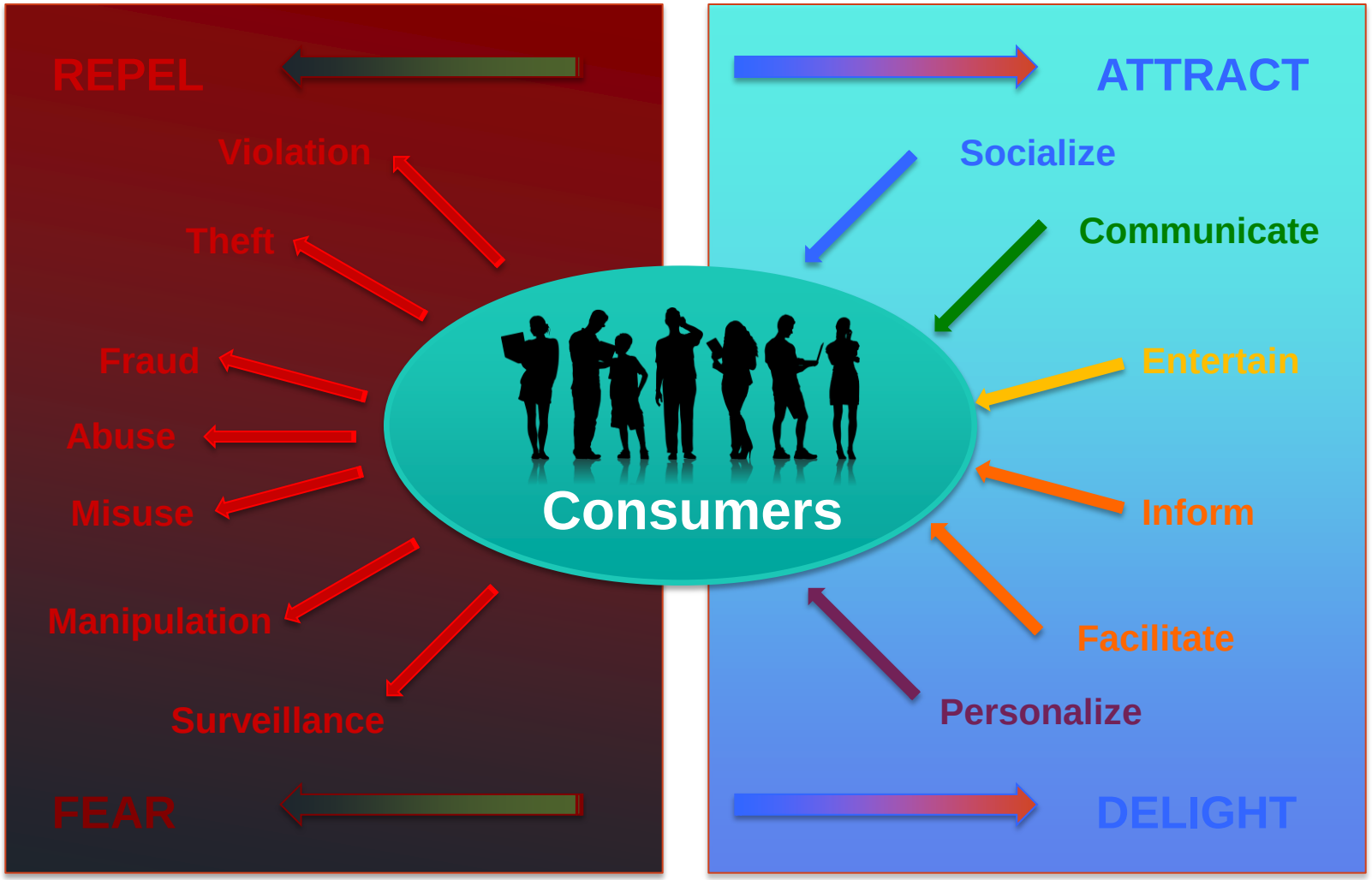
1. Trust and the Internet
2. Data Protection and Privacy
3. Data Protection Regimes and Recent Developments
4. E-Privacy
5. Cybersecurity
6. Concluding Thoughts

SQUIRE PATTON BOGGS

1. Trust and the Internet

1. Trust and the Internet

SQUIRE PATTON BOGGS



1. Trust and the Internet (cont'd)

SQUIRE PATTON BOGGS

Conflicting Agendas

Globalization	⟷	Local Norms
Hyperconnectivity	⟷	Mindfulness
Anonymity	⟷	Responsibility
TMI	⟷	Transparency/Notice
Opt-out	⟷	Opt-in
Business Innovation	⟷	Data Protection
Access	⟷	Personal Security
Net Control	⟷	Net Neutrality/Open Internet
State Security	⟷	Individual Freedoms
Data Retention	⟷	Encryption/Tokenization
Reasonable expectation of privacy/context	⟷	Privacy as fundamental human right

Internet or Splinternet ?

1. Trust and the Internet (cont'd)

SQUIRE PATTON BOGGS

Consumer Concerns Related to Online Privacy

How concerned are you about:	% who agree
Someone breaking into your internet account or e-mail?	72%
Information you provided for one purpose being used for another purpose online?	67%
Your reputation being damaged by what someone posts online?	62%
Your views or behaviours being misunderstood online?	57%

Source: 2014 World Economic Forum, "The Internet Trust Bubble: Global Values, Beliefs and Practices" (Dutton, Law, Bolsover & Dutta)

SQUIRE PATTON BOGGS

2. Data Protection and Privacy

2. Data Protection and Privacy

(1) What is "Personal Data" ?

- Broad definition:

Any information relating to an identified or identifiable natural person (*i.e.*, one who can be identified, directly or indirectly, in particular by reference to **an identifier** such as a **name**, identification number, **location data**, **unique identifier** or to one or more factors specific to the physical, physiological, **genetic**, mental, economic, cultural or social or **gender** identify of that person.

- Draft EU Data Protection Regulation (Art. 4(2))

2. Data Protection and Privacy (cont'd)

SQUIRE PATTON BOGGS

(1) What is "Personal Data" ? (cont'd.)

- Narrow definition

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, *when either the name or data elements are not encrypted*:

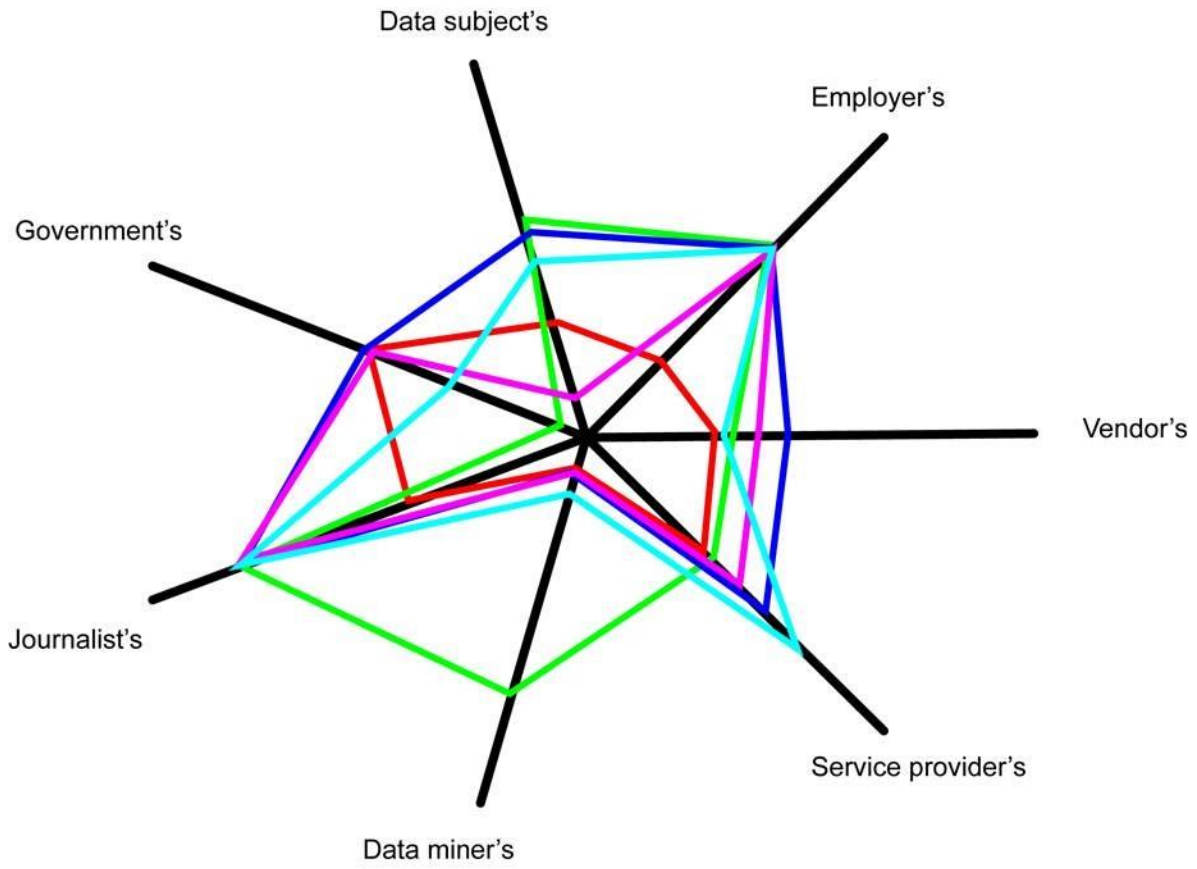
- Social security number;
- Driver's license number; or
- Account or credit card number combined with security code, access code or password allowing access to a financial account

  - California Data Breach Notification Law, SB 386.

2. Data Protection and Privacy (cont'd)

SQUIRE PATTON BOGGS

(2) Balance of Interests



(2) Data Protection and privacy (cont'd) – *Importance of Context*

SQUIRE PATTON BOGGS

Objective variables

Type of data

What type of data is it?

Type of entity

Who is accessing it?

Device context

What kind of device is used?

Collection method

How is the data collected?

Data usage

How is the data used?

Subjective variables

Trust in service provider

What is the user's relationship with the SP?

Value exchange

How do users perceive the benefits from the use of their data?

Source: Microsoft

SQUIRE PATTON BOGGS

3. Data Protection Regimes and Recent Developments

Risk Assessment for Selected Jurisdictions

SQUIRE PATTON BOGGS

Region / Country	Admin / Legal Compliance	Human Resources	Data Transfers	Marketing	Security	Data Subject Rights	Powers & Penalties	Overall Score
Australia	1	1	2	3	3	2	2	**2**
France	5	4	4	4	3	5	5	**4.5**
Germany	4	4	4	5	4	5	3	**4**
Hong Kong	2	3	1	4	3	3	3	**3**
India	1	1	1	0	4	1	1	**1.5**
Japan	3	3	3	3	4	3	3	**3**
Russia	3	4	3	2	4	4	2	**3.5**
UK	2	3	2	3	4	3	3	**3**

Source: Data Guidance

(1) Overview of Data Protection Regimes

SQUIRE PATTON BOGGS

Region / Country	Admin / Legal Compliance	Human Resources	Data Transfers	Marketing	Security	Data Subject Rights	Powers & Penalties	Overall Score
Argentina	2	2	2	2	2	2	2	**2**
Chile	0	1	0	1	0	3	2	**1**
Columbia	1	1	1	0	1	2	1	**1**
Mexico	1	2	2	2	2	2	3	**2**
Peru	2	2	2	2	2	2	2	2
Uruguay	2	2	2	2	3	2	2	**2**

Source: Data Guidance
Note that whilst not yet having an impact on the scores, the Argentinian DPA showed a much increased level of activity in 2013

(1) The EU

(1) The EU

SQUIRE PATTON BOGGS

Privacy as a human right

- In Europe, privacy is a fundamental right….
  - Article 8 of the Charter of Fundamental Rights of the EU expressly recognises that all citizens of the EU have a fundamental right to privacy
- In contrast to US practice, protection of personal data is the rule and not the exception
- Individuals are generally viewed as having the right to be informed of whether and how data about them is collected, processed and transferred, including in the workplace
  - In some cases, their explicit consent is required for these activities
- The EU approach is “horizontal” – general principles apply across all sectors and types of activities, by contrast with the “vertical” sector-specific approach followed to date in the US

(1) The EU (cont'd)

SQUIRE PATTON BOGGS

Draft EU Regulation: Status

- Originally proposed by the European Commission on 25 January 2012
- On 12 March 2014, the European Parliament voted in favour of the "Compromise Text" of the draft Regulation
  - To become law, the draft Regulation must be agreed with EU Council of Ministers
  - Regulation is highly controversial and unlikely to be approved before 2015
- Some Member States still trying to block the draft Regulation
  - Pushing for a watered-down Directive (UK, Sweden, Czech Republic and Hungary)

1. The EU (cont'd)

SQUIRE PATTON BOGGS

Draft EU Regulation: Extra-territorial effects

- Applies to controllers and processors even with no physical presence in the EU if they process personal data in connection with:
  - provision of goods or services to data subjects in the EU; or
  - monitoring of data subjects in the EU

- If a non-EU government/court requires a company (e.g. a search engine, cloud provider) to disclose EU personal data, the data controller/processor must:
  - notify the data protection authority without undue delay;
  - obtain prior authorization for the disclosure/transfer; and
  - inform the relevant data subject(s)

  (unless mutual assistance or other international treaty applies)

- Conflict of laws!

(1) The EU (cont'd)

SQUIRE PATTON BOGGS

Draft EU Regulation: Data processors (the cloud)

- Definitions of "data processors" and "data controllers" remain much the same under the draft EU Regulation

- Controller: "determines, alone or jointly with others, the purposes and the means of the processing of personal data"
  - Currently the sole focus of EU data protection rules
- Processor: "processes personal data on behalf of the controller"
  - Cloud providers usually consider themselves 'processors'
  - Subject only to contractual obligations imposed by controllers
- New obligations imposed directly on data processors, e.g.:
  - Both controllers and processors must maintain regularly updated documentation
  - Requirement for a security policy and to implement appropriate and state-of-the-art technical and organisational measures
  - Data protection officer: obligation on businesses processing data of 5000+ individuals

(1) The EU (cont'd)

SQUIRE PATTON BOGGS

Draft EU Regulation: "Right to be forgotten" / "right to erasure"

- Data subject right to obtain:
  - from the controller erasure of data relating to them, and
  - from third parties (processors) erasure of links to, or copy/replication of, such data

    WHERE
  - Data no longer necessary for purpose for which originally collected/processed;
  - Data subject withdraws consent if consent was basis for collection, or storage period has expired and no legal ground for processing remaining;
  - A court in the EU has ruled as final and absolute that the data must be erased; or
  - Data has been unlawfully processed
- Erasure "without delay" unless retention is necessary for reasons of freedom of expression, public health interest, to comply with legal obligations, etc.
- Restricted processing instead of erasure required in specified circumstances
  - e.g., accuracy is contested and must be verified; or if storage technology installed pre-Regulation does not allow erasure

(1) The EU (cont'd)

SQUIRE PATTON BOGGS

Comparison: Decision of the EU Court of Justice on Google Search*

- Q: whether Google's search engine acts a "data controller", and thus is required to comply with the existing data protection regime in Spain

- CJEU: Google's search engine business is that of a "data controller"
  - Google determines the purposes and means of the processing of personal data – *i.e.*, the search activity
  - Would be contrary to the objective of ensuring complete protection of data subjects for a search engine operator not to fall under the definition

- CJEU: Google processes personal data when it:
  - '*collects' data which it subsequently 'retrieves', 'records' and 'organises'…'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results*

- Draft EU Regulation clarifies that the right to erasure would apply to any data controller around the world offering goods/services in the EU

**Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*

(1) The EU (cont'd)

SQUIRE PATTON BOGGS

Comparison: Decision of the EU Court of Justice on Google Search*

- Q: whether Google's search engine acts a "data controller", and thus is required to comply with the existing data protection regime in Spain

- CJEU: Google's search engine business is that of a "data controller"
  - Google determines the purposes and means of the processing of personal data – *i.e.*, the search activity
  - Would be contrary to the objective of ensuring complete protection of data subjects for a search engine operator not to fall under the definition

- CJEU: Google processes personal data when it:
  - '*collects' data which it subsequently 'retrieves', 'records' and 'organises'…'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results*

- Draft EU Regulation clarifies that the right to erasure would apply to any data controller around the world offering goods/services in the EU

**Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*

(1) The EU (cont'd)

SQUIRE PATTON BOGGS

Data Portability

- The right to data portability has been added to the right of data subjects to access their personal data.
- Electronically processed data should be provided to data subjects on request "in an electronic and interoperable format" to facilitate moving data between service providers.
- Where technically feasible and available, the data should be transferred directly from controller to controller at the request of the data subject.

(1) The EU (cont'd)

SQUIRE PATTON BOGGS

Privacy by Design

- Privacy by design/default obligations will apply to both data controllers and processors, including cloud providers:

> " Having regard to the state of the art, current technical knowledge, international best practices and the risks represented by the data processing, the controller and the processor, if any, shall, both at the time of the determination of the purposes and means for processing and at the time of the processing itself, implement appropriate and proportionate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject … Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data …"

(1) The EU (cont'd)

SQUIRE PATTON BOGGS

Profiling – Big Data

- Notices about profiling must be highly visible and individuals must have the opportunity to object.

- Where profiling significantly affects an individual's rights, it will only be allowed: (1) where the individual's explicit consent is obtained; (2) where provided for by law; or (3) where necessary to conclude or perform a contract.

- Profiling based solely on sensitive data or profiling which has the effect of discriminating against individuals (such as that based on race or political opinions) is prohibited.

- Profiling based on pseudonymous data is acceptable provided the data cannot be linked to a specific individual.

(1) The EU (cont'd)

SQUIRE PATTON BOGGS

Impact Assessments and DPOs

- Obligation to carry out a privacy impact assessment and appoint a data protection officer (DPO) in cases where:
  - Personal data relating to more than 5,000 data subjects is processed during any consecutive 12 month period; or
  - The processing relates to sensitive data, location data, data relating to children or employees in large filing systems.
- DPOs must be appointed for at least 4 years (employees) or 2 years (contractors).

(1) The EU (cont'd)

SQUIRE PATTON BOGGS

International Data Transfers under the Current EU Framework

There are various ways in which personal data can be transferred outside of the EEA in accordance with the current EU data protection framework:

- Certain conditions are met, such as where the unambiguous consent of the data subject is obtained, or where the transfer is necessary for the performance of the contract between the data subject and the controller

- An "adequate level of protection" in the country of import (EU finding):
  - Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Isle of Man, Jersey, US (Safe Harbor)

- Model Clauses – standard contractual clauses approved by the EU

- Binding Corporate Rules (BCRs)

- Self-Certification under the EU/US Safe Harbor framework

(1) The EU (cont'd)

SQUIRE PATTON BOGGS

Draft EU Regulation: International data transfers

- Transfers to third countries (including the US) can only be effected if one of the following applies:
  - Both controller and recipient have a valid European Data Protection Seal (EDPS)
  - An adequacy decision applies or the recipient is Safe Harbor certified
    - BUT existing adequacy decisions will expire 5 years after entry into force of the Regulation AND in any event Safe Harbor is currently being reassessed (see later)
  - Standard clauses adopted by a competent authority (*e.g.*, EU Model Clauses)
    - BUT existing standard clauses will expire 5 years after entry into force of the Regulation
  - Approved binding corporate rules or binding processor rules (proposed by A29WP)
    - BUT existing approvals will expire 2 years after entry into force of the Regulation
  - Informed consent of the data subject, or transfer is necessary for the performance of the contract between the data subject and the controller (but will not legitimise routine/systematic transfers) [among other justifications]

(1) The EU (cont'd)

SQUIRE PATTON BOGGS

US-EU Safe Harbor

- Draft Regulation allows for "sunset" of existing authorisation procedures for international data transfers (including Safe Harbor) after 5 years or sooner if Commission decides
  - Legal uncertainty for long-term cloud and other outsourcing agreements involving international transfers from the EU to the US

- November 2013: European Commission made 13 recommendations to the US-EU Safe Harbor framework to restore the trust in US-EU data flows:
  - Making Safe Harbor more transparent (e.g. requiring self-certified companies to publically disclose their privacy policies);
  - Ensuring that all Safe Harbor self-certified companies offer an Alternative Dispute Resolution mechanism in their privacy policy;
  - Actively enforcing and auditing compliance with the Safe Harbor scheme;
  - Clarifying the circumstances under which US authorities may access EU personal data processed by a Safe Harbor self-certified company.

(1) The EU (cont'd)

SQUIRE PATTON BOGGS

Safe Harbor (cont'd)

- Commission had expected implementation of Recommendations by summer 2014…
  - Then decide whether to maintain, modify or revoke Safe Harbor framework
- 12 March 2014, European Parliament resolution calling for immediate suspension of Safe Harbor
  - However, underlying agreements entered into by Commission – only Commission has the power to decide the future of the Safe Harbor framework
- US/EU Transatlantic Trade and Investment Partnership ("TTIP") currently being negotiated
  - Debate over whether to include standards for EU-US data transfers
    - Many US tech companies hoping for the streamlining of international transfer rules
  - EU Commission resisting inclusion
    - Data protection is a "fundamental right and not negotiable" (Commissioner Reding)
  - Snowden revelation have had significant impact on the debate

(1) The EU (cont'd)

SQUIRE PATTON BOGGS

Draft EU Regulation: Sanctions

- Sanctions:
  - Originally proposed fines of up to EUR 1 million or 2% of turnover
  - Snowden effect: latest draft increases these sanctions up to EUR 100 million or 5% of turnover
  - Other sanctions include warnings and regular periodic data protection audits

- Latest draft also includes a private right of action for individuals who have suffered damage (including non-pecuniary damage) as a result of violations

(2) Russia

(2) Russia

SQUIRE PATTON BOGGS

Overview

- Data protection provided for in general data protection law, the Information, IT and Information Protection Law and sectoral laws (*e.g.*, labour code)
- Personal data: any information directly/indirectly related to identifiable individual
- International transfers: recipient state must provide adequate protection
- Consent of individual is required for processing personal data

(2) Russia

Key change to Data Protection Laws: effective from 1 Sept 2016

- Personal data collected in Russia (including via the Internet) must be stored in data centers located in Russia
  - DPA has right to block internet sources in Russia which are used to process personal data in breach of the rules
- Apparent intention to target internet/telecom companies, BUT broad definition of “operator” appears to cover most (if not all) companies
  - Russian subsidiary of company would be required to set up local servers to host Russian personal data
  - International companies would need to segregate data by country of origin
- Expectation that transfers to servers abroad (mirroring) will be permitted with consent

SQUIRE PATTON BOGGS

4. E-PRIVACY

4. E-Privacy

SQUIRE PATTON BOGGS

(1) EU E-Privacy Directive (2002) -- Highlights

- **Confidentiality of communications** and related traffic data must be protected.
- **Prohibition against "listening, tapping**, storage, interception or surveillance of public communications and related traffic data . . .
  - without user's consent
  - unless legally authorized to safeguard national security, defense, public security, prosecution of criminal offenses or unauthorised use of electronic communications.

4. E-Privacy

SQUIRE PATTON BOGGS

(1) EU E-Privacy Directive (2002) – Highlights (cont'd)

- **Traffic data** relating to subscribers/users that is processed or stored by public communications service or network providers:
  - must be erased or anonymized when no longer needed for transmission or billing;
  - may be used to market or provide value added services if the user gives prior consent;
- **Location data** relating to users of public communications (other than traffic data) must be anonymized before processing unless . . .
  - Proper notice of purpose/scope/transfer provided in advance, and
  - user consents.

4. E-Privacy (cont'd)

SQUIRE PATTON BOGGS

(1) EU E-Privacy Directive (2002) (cont'd)

- Public communications providers must:
  - take appropriate technical and organizational measures to safeguard security;
  - allow security audit of systems; and
  - notify national authority and affected individuals in the event of data breach.

4. E-Privacy (cont'd)

SQUIRE PATTON BOGGS

(2) Concerns raised by differential regulation of e-privacy

- "Value added services" include hot new applications and content.
- Telco and ISP margins are declining and value added services are viewed as lucrative new source of revenue.
- "Over-the-top" providers (OTTPs) compete head-on with telcos and ISPs.
- But, OTTPs are not subject to the EU's e-Privacy rules if they do not fall under the definition of "public communications" provider.

4. E-Privacy (cont'd)

SQUIRE PATTON BOGGS

- Instead, OTTPs are subject to general DP Directive, so . . .
  - use of data may be deemed necessary to perform contract
  - consent may be implied rather than explicit
  - opt-out versus opt-in
  - no general data breach notification obligation.

(3) EU Data Protection Regulation, if adopted in its current form, will reduce (but not eliminate) the differences in regulatory treatment between telcos and OTTPs.

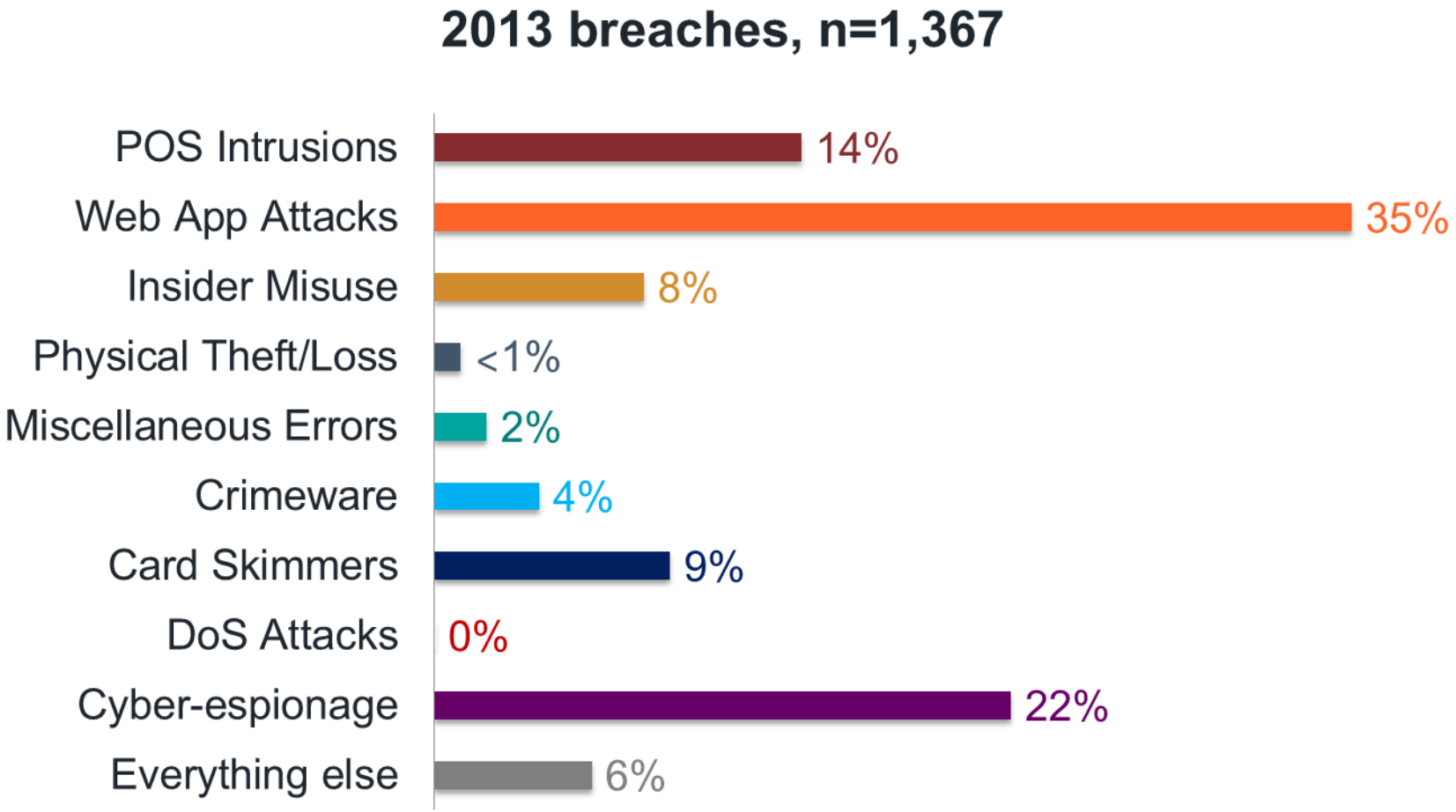
SQUIRE PATTON BOGGS

5. CYPERSECURITY

5. Cybersecurity

SQUIRE PATTON BOGGS

(1) Top cyber risks in 2013



Verizon: 2014 Data Breach Investigations Report

5. Cybersecurity

SQUIRE PATTON BOGGS

(2) Internet as "The Fourth Utility"

- Information Technology Sector (including the Internet) is one of 16 sectors classified as critical infrastructures by US Dept. of Homeland Security.
- Establishment of DHS "Office of Cybersecurity & Communications".
- FCC Chairman Wheeler has recently announced new "Cybersecurity Paradigm" (June 2014) – pressing industry to take the lead and collaborate on developing more secure systems to keep the Internet safe.
- EU Digital Agenda sets our 14 actions to improve cybersecurity readiness, including network of national Computer Emergency Response Teams (CERTs) covering all of Europe.

5. Cybersecurity

SQUIRE PATTON BOGGS

(3) Cyber hacking incidents have led to:

- Massive litigation, *e.g., Target*
  - December 2013 hack into database containing customer names, addresses and credit card details
  - Delays in detecting and reporting the breach
  - Lawsuits by banks and customers for negligence, violating customer's privacy rights, breaching fiduciary duties, and failing to disclose breach in timely manner
  - Resignations of CEO and CIO
- Rise of cyber insurance
- Calls for legislation at federal level in US.

5. Cybersecurity

SQUIRE PATTON BOGGS

(4) Data Retention and Surveillance

- The EU Data Retention Directive (2006)
  - Covers many types of "non-content" data, *e.g.*:
    - subscriber data,
    - date/time/duration of communications,
    - Internet log-in/log-off data
    - type of communication,
    - type of equipment used,
    - Internet email and telephony data, and
    - location (mobile cell) data.
  - Authorizes derogation from Data Protection Directive for providers of publicly available electronic communications services.
  - Purpose was to harmonize retention requirements across the EU but allows Member States to mandate retention for between 6 months and 2 years
  - Data must be made available to "competent national authorities" for purpose of investigating and prosecuting "serious crime" following procedures set by national law.

5. Cybersecurity

SQUIRE PATTON BOGGS

(4) Data Retention and Surveillance (cont'd)

- The EU Data Retention Directive (2006) (cont'd)
  - Directive was controversial, implemented in different ways by Member States and subject to constitutional challenges at national level.
- EU Court of Justice issued decision in April 2014 in the case of *Digital Rights Ireland* and *Seitlinger:*
  - CJEU's Decision followed requests from the Irish High Court and the Austrian Constitutional Court.
  - Decision invalidates the Data Retention Directive on various grounds, concluding that although the objective of combatting serious crimes may justify retention of some communications data, ***the Directive interferes disproportionately with the fundamental rights to privacy in ways that are "wide ranging, and particularly serious***."

5. Cybersecurity – EUCJ's

SQUIRE PATTON BOGGS

(4) Data Retention and Surveillance (cont'd)

- Highlights of the CJEU's rationale:
  - The metadata in question, even if not content, can provide very precise information on the private lives of individuals.
  - The Directive provides for blanket retention without regard to the types of data or any differentiation based on linkage of individuals with serious crimes.
  - It leaves the term "serious crime" undefined.
  - It provides inadequate safeguards against risk of abuse.
  - It fails to ensure irreversible destruction of data at end of retention period.

5. Cybersecurity

SQUIRE PATTON BOGGS

(4) Data Retention and Surveillance

- UK Reaction
  - Emergency legislation ("DRIPA") was enacted by Parliament in July 2014 in just 3 days to reaffirm the original data retention obligations on communications providers following the CJEU's decision invalidating the Data Retention Directive.
  - DRIPA also expanded the pre-existing measures in some respects (jurisdiction).
  - Legal challenges have already been lodged against DRIPA on the basis that the CJEU's concerns have not been addressed.

5. Cybersecurity

SQUIRE PATTON BOGGS

(5) "The Snowden Effect" – Global reaction to NSA/GCHQ and other surveillance tactics, and complicity of telecoms and Internet providers

- US – Obama Administration calls for US Congress to adopt safeguards to limit NSA bulk data collection activities (March 2014).
  - House of Representatives passed bill by vote of 303 to 121 to limit NSA data collection (May 2014)
  - Even tougher Senate bill reportedly ready for passage.
- EU – TTIP effects, Safe Harbor warnings and changes to EU Data Protection Regulation.

SQUIRE PATTON BOGGS

6. CONCLUDING THOUGHTS

6. Concluding Thoughts

SQUIRE PATTON BOGGS

- Is data the fuel that runs the Internet primarily because consumers do not expect to pay?
- Can consumer consent be “informed” in such a complex ecosystem?
- Is the Internet at risk of becoming so polluted that use is seriously discouraged?
- Is business doing enough to (re)build trust in the Internet?
- Is government part of the solution or part of the problem?
- Does the law really matter?

➲ Is Telex back to the future?