Software Requirements

L11: Legal Requirements and Compliance

Dr. Farnaz Fotrousi, Prof. W. Maalej

Overview

1 **Legal Requirements**

2 **Security & Privacy Requirements**

Motivation

- Companies are governed by numerous legal obligations
- Violations can lead to high fines or even prison sentence
- Examples:
  - Microsoft Browsers case vs. European Commission
  - Right to be forgotten

Legal Obligation Example: Microsoft vs. European Commission

- In Dec. 2009 the European Union agreed to allow **competing browsers**, with Microsoft letting users to choose one of the popular products listed in random order
- Microsoft **dropped this feature** in Windows 7 Service Pack 1 in February 2011 (absent for 14 months)
- In March 2013 the European Commission fined Microsoft **€561 million** to deter companies from reneging on settlement promises

Legal Obligation Example: „The Right to Forget“

- In May 2014, the European Court of Justice ruled against Google in Costeja
- The case was brought by a Spanish man who requested the removal of a link to a digitized 1998 article in a newspaper about an auction for his foreclosed home, for a debt that he had subsequently paid
- The court ruled in Costeja that search engines are responsible for the content they point to
- Google was required to **comply** with EU data privacy laws
- On its **first day** of compliance Google received **12,000 requests** to remove personal details from its search engine

12,000 entries: Google flooded with Europeans' 'right to forget' requests

Published time: June 01, 2014 12:12

Get short URL

Reuters / Francois Lenoir

Legal Requirements & Compliance

- **Legal Requirements** are constraints requirements imposed by law and concerned e.g. with licensing, regulation, and certification issues

- **IT Compliance** is concerned to adhere the legal, contractual, or corporate requirements in the field of IT

Types of Legal Requirements

- Licensing
- Certification
- Laws and statutes
- Standards
- Guidelines (Branch, Company)
- Contracts with third parties
- Safety regulations
- Privacy policies
- …

Main Activities for Analysts

- **Determine** the applicable **regulations**
- Create policies and requirements necessary to **achieve compliance** with those regulations
- Assist stakeholders in **understanding the regulations**
  - What is allowed?
  - What is not allowed?
- **Monitor** the compliance tthroughout the software lifecycle

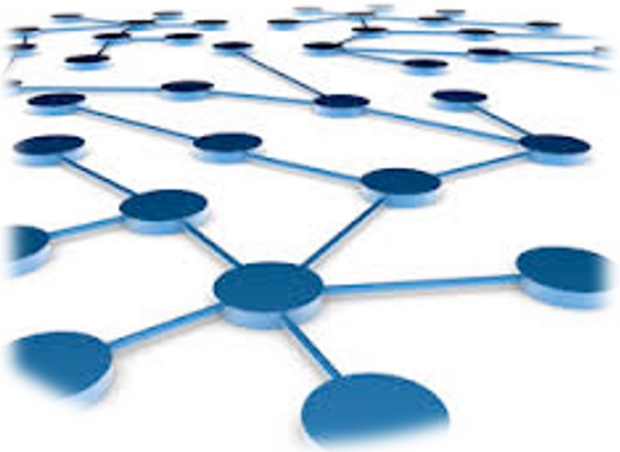
The Nature of Regulations

- Regulations are usually structured in **hierarchical** documents
- They **evolve** over time
  - New regulations emerge that **complement, contradict, or overlap** with existing ones
- Coexistence of two forms of law
  - Statutory law: the law in force
  - Case law: the courts' interpretations of the law

Challenges in Handling Legal Requirements

Cross-references

- Frequent references to other **sections** within a given legal text and to **pieces of law**
- **Time** needed to read and understand legal texts



Understanding legal texts

- Legal texts have a large corpus of **domain-specific definitions and acronyms** that make them difficult to understand

Ambiguities

- Legal requirements are hard to identify as legal texts are usually ambiguous when a single word or phrase may be interpreted in two or more ways.

Example: Ambiguity of Natural Language

Requirement:

- "Shut off the pumps if the water level remains above 100 meters for more than 4 seconds"

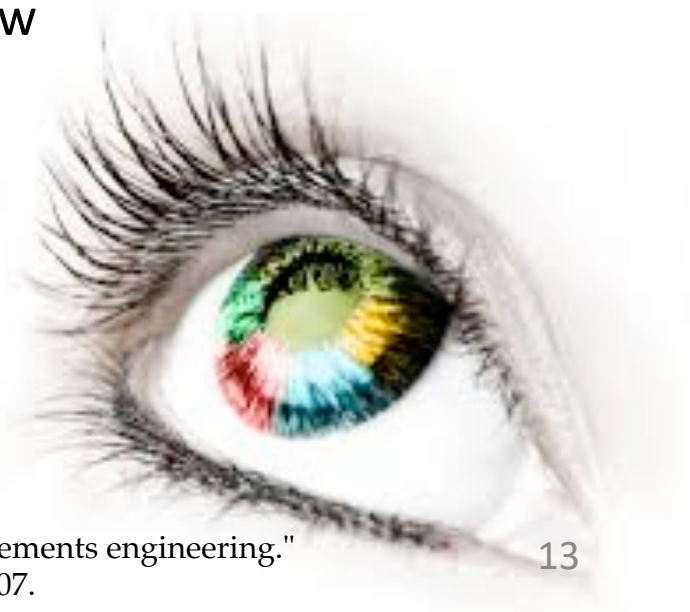
Interpretations

- "Shut off the pumps if the *mean* water level over the past 4 seconds was above 100 meters"
- "Shut off the pumps if the *median* water level over the past 4 seconds was above 100 meters"
- "Shut off the pumps if the *root mean square* water level over the past 4 seconds was above 100 meters"
- "Shut off the pumps if the *minimum* water level over the past 4 seconds was above 100 meters"

Supporting Requirements Analysts in Legal Contexts

Goal: a system that supports the analysis of regulatory texts for requirements, design, and compliance monitoring

- Identification of **relevant** regulations
- **Annotation** of regulatory statements
- Classification of regulations with **metadata**
- **Prioritization** of regulations and exceptions
- Management of **evolving** regulations and law
- **Traceability** between references and requirements
- Data dictionary and **glossary** to ensure consistency
- **Navigation** and searching



Otto, Paul N., and Annie I. Antón. "Addressing legal requirements in requirements engineering." *15th IEEE international requirements engineering conference (RE 2007)*. IEEE, 2007.

Overview

1 Legal Requirements

2 **Security & Privacy Requirements**

Security Requirements

- Authentication
  - Block **unauthorized access** to system functions or data
- Confidentiality
  - Protect software from **malware** attacks
- Availability
  - Protection of **denial-of-service** attacks
- Integrity
  - Error tolerant

Security Requirements Knowledge

Explicit

- Documented (e.g. security standards, checklists, vulnerability bulletins, etc.)
- Usually easy to access

Tacit

- Security experts with experience and tacit knowledge about security issues
- Hard to elicit and access

Security Requirements Examples

- Functional Security Requirements
  - After 3 consecutive failed login attempts within 20 seconds, the account shall be locked within 3 minutes
- Non-Functional Security Requirements
  - The system shall have integrity protection mechanisms for audit logs
  - The application must not accept invalid URLs.
  - The development processes must comply with SSE-CMM capability level 3 or above.

Security Requirements Guidelines

- User **authorization** or **privilege** levels
  - User, Guest User, Administrator, Auditor, etc.
- User **access control**
  - Roles and permissions
- **Data privacy**
- Deliberate data destruction, corruption, or theft
- Protection against viruses, worms, spyware, rootkits, etc.
- Firewall and other **network security** issues
- **Encryption** of secure data
- **Audit trails** of performed operations and access attempts

Safety vs. Security

- **Security** is concerned with the protection of the system and users from harm
- Security focuses on threats coming from outside the system

- **Safety** is concerned with the protection of the life, health, and natural environment from any damage that the system may cause
- Safety focuses on unintentional event
- Example: “The system shall not cause more than X safety incidents per passenger mile traveled.”

Privacy Requirements

Privacy is…

"**right** to be left alone" [Warren and Brandeis, 1890]

"**freedom** from unauthorized intrusion" [Merriam-Webster]

Privacy requirements are mainly about the needs on having some control over how to protect personal information while collecting and using.

privacy

All Images News Videos Maps More

About 12 120 000 000 results (0,52 seconds)

https://privacy.com

Privacy - Smarter Payments

Make a unique debit card number for every single purchase online with ju

again about credit card breaches, shady merchants, or sneaky ...

Log in · Privacy · Sign Up · Virtual Cards

Google

security

All Images Maps News Videos More

About 6 190 000 000 results (0,70 seconds)




Security is freedom from, or resilience against, potential harm (or other unwante
change) caused by others. Beneficiaries (technically referents) of **security** may b
persons and social groups, objects and institutions, ecosystems or any other enti
phenomenon vulnerable to unwanted change.

https://en.wikipedia.org › wiki › Security

Security - Wikipedia

safety

All Images Maps Videos News More

About 3 340 000 000 results (0,93 seconds)

Dictionary

Search for a word

safety

/ˈseɪfti/

Your Facebook privacy settings are about to change. Again.

BY **BRIAN FUNG** April 8 at 5:45 pm

E.g. EU data protection directive

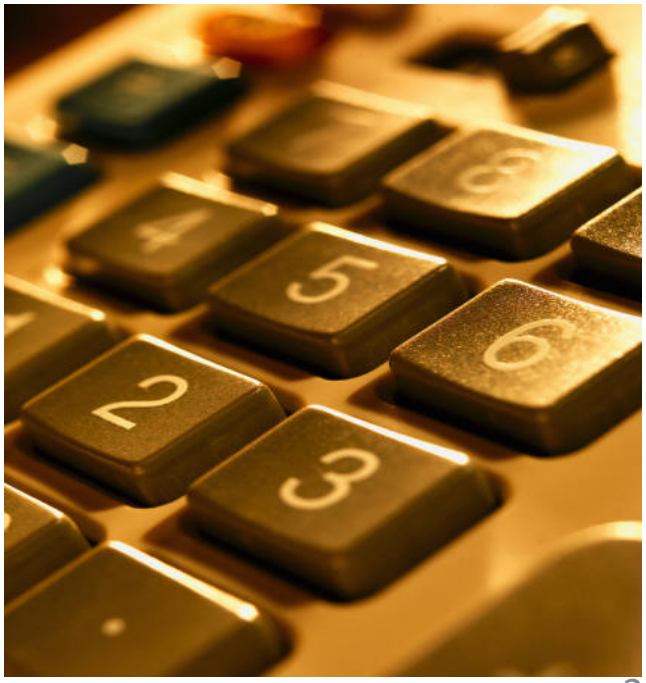
EU Legal Principles of Data Protection 2/4

1. Purpose Limitation

Explicit limitation of the secondary use of personal data, incompatible with the intended purpose

2.Data Minimization

The processing of personal data must be necessary and proportionate



EU Legal Principles of Data Protection 4/4

3.Transparency

The users must be aware about the data collection and processing

4.Data Security

The personal data should be safeguarded, as appropriate to the sensitivity of the information

Purpose Limitation Requirements

- App developers should describe the **purpose** of their apps and the **data processing operations** carried out by their apps in a well-defined and comprehensible way
- Should be explicit: the user must understand the reasons behind the processing of the data
- Should be legitimate i.e. compatible with all legal principles of applicable law, e.g. non-discrimination principles
- App store description can be a first indicator for the usage of personal data

Data Minimization Requirements

- The collection and the use of personal data should be limited to what is reasonably necessary to achieve the purpose
- Developers must find out whether the app needs to process personal information at all
- They should carefully consider the relevancy of the personal data they tend to process
- When users perceive a potential privacy violation, they opt-out of the app, rather then to change privacy settings

Transparency Requirements

- Users must be aware of the processing of their data, including the disclosure of their data to third parties
- App developers must ensure that their design does not conceal the nature and extent of potential nor actual disclosure of information through or outside the system
- Current state in the app market
  - In 2012 only 61% of the top 150 apps provided a privacy policy that sufficiently explained to the users which data were collected through the app, and how it was processed
  - Some applications claim that no personal data is processed, even they process user ids, or their devices' ids

Data Security Requirements

- Poor security measures for storage and transfer of user data cause additional risks for the protection of the users' personal data
- Insufficient information security often leads to unauthorized access or unauthorized processing of personal information
- Information about users should be protected both in transit and during storage
- Encryption should be used as a default. All files and all communication should be encrypted
- User information can never be transmitted in clear text nor passwords can be stored in clear text
- It is important to note that the encryption of data is not equal to the anonymization of data
- Only anonymized data is excluded from the scope of the data protection legislation

Privacy Concerns

Data Aggregation

Aggregation of user data over long period of time

Data Distortion

Misrepresentation of the data or user intent

Data Sharing

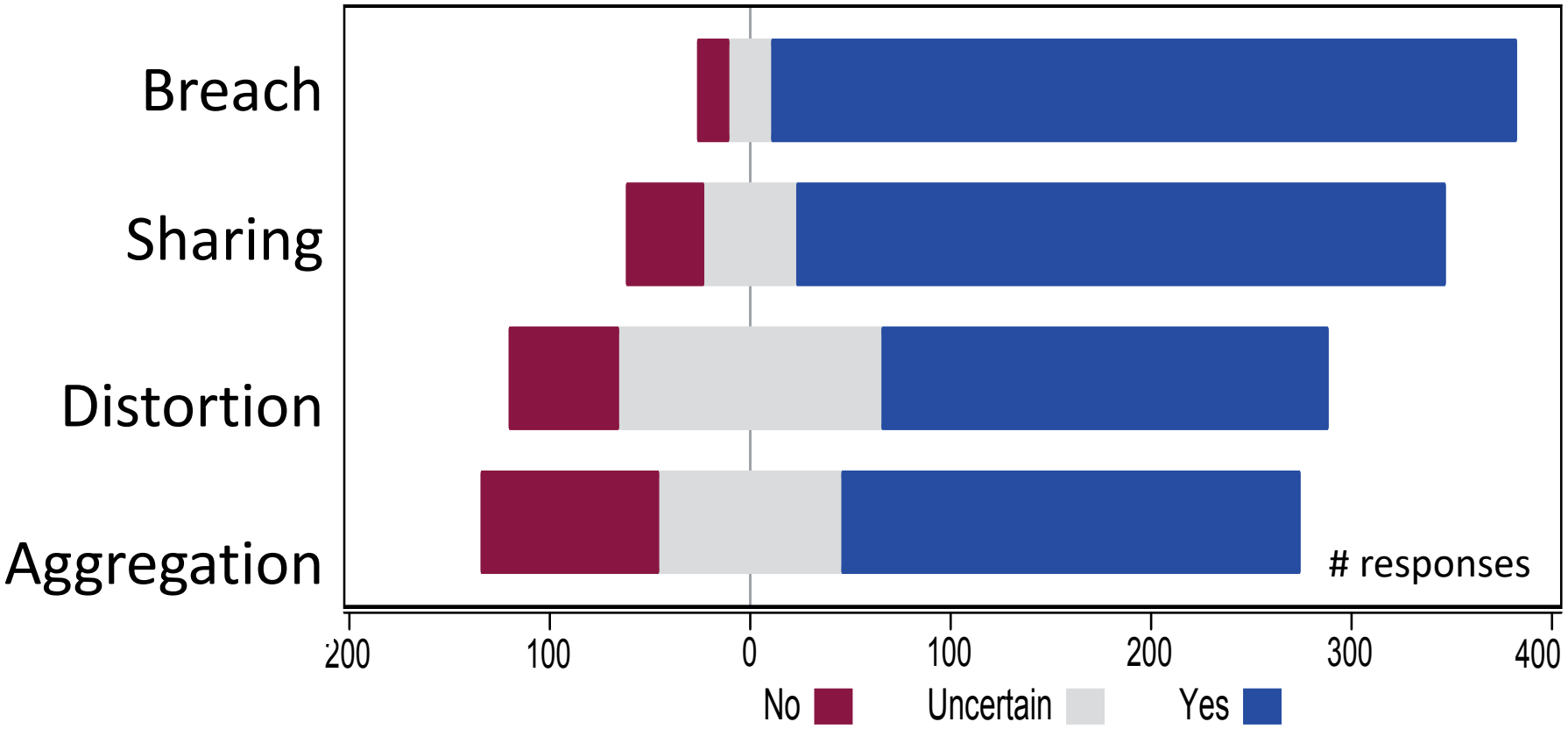
Collected data given to third parties e.g. for advertising

Data Breaches

Malicious users get access to sensitive data

Everybody is Talking about Privacy

What Increases Privacy Concerns?

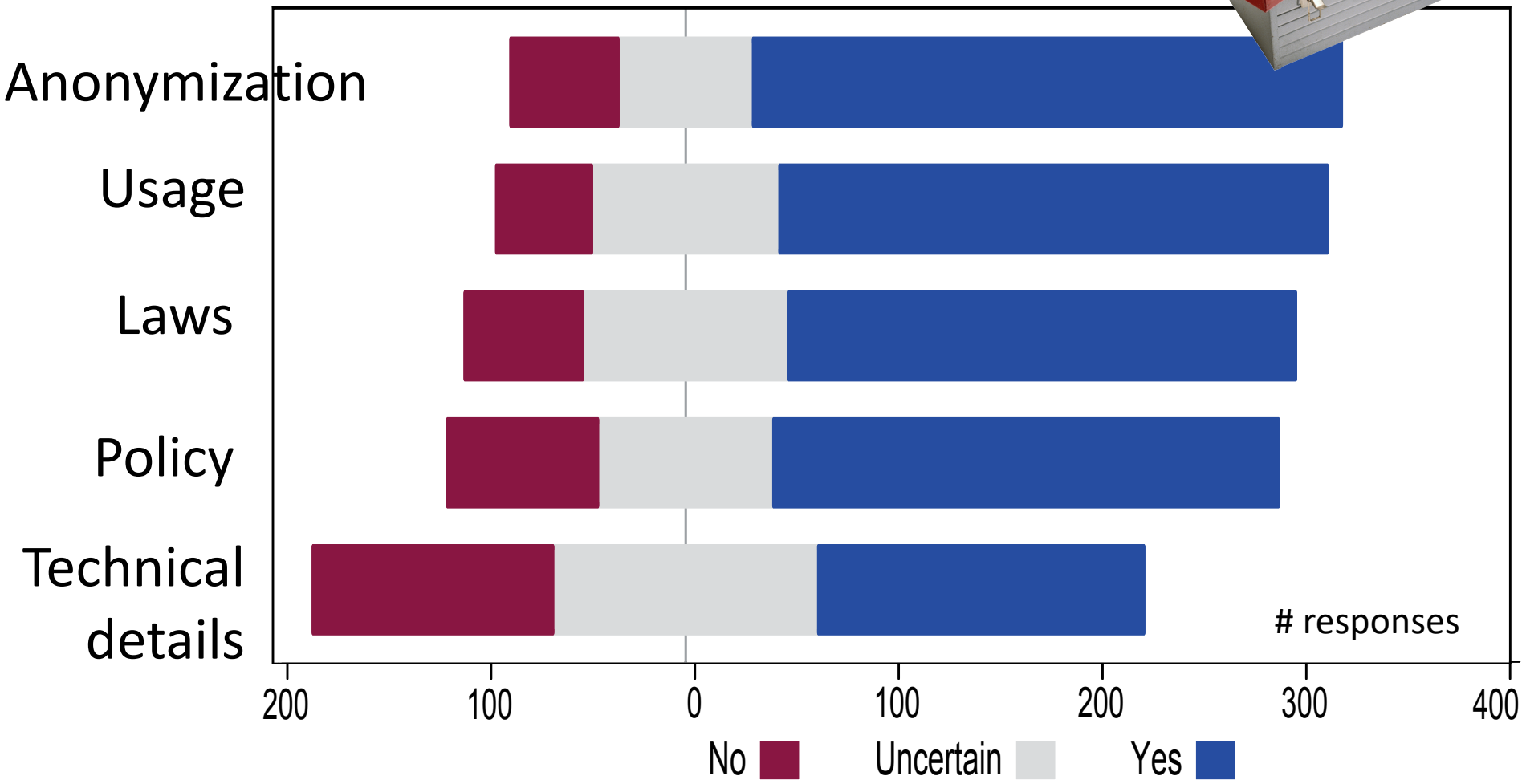


Sheth, Swapneel, Gail Kaiser, and Walid Maalej. "Us and them: a study of privacy requirements across North America, Asia, and Europe." *Proceedings of the 36th International Conference on Software Engineering*. 2014.

Reducing Privacy Concerns

- **Privacy Policy** and license agreements
- **Privacy Laws** e.g. HIPAA or EU Privacy Directive
- **Anonymization** removing personal identifiers
- **Technical Details** e.g. encryption algorithm
- **Details on Usage** how different data are used

What Reduces Privacy Concerns?



Sheth, Swapneel, Gail Kaiser, and Walid Maalej. "Us and them: a study of privacy requirements across North America, Asia, and Europe." *Proceedings of the 36th International Conference on Software Engineering*. 2014.

Towards a Privacy Framework

- Anonymization
- Data usage details
- Fine-grained control over data
- Metadata and interaction data first
- Time and space limited storage
- Privacy “licenses”

Summary

1. Analysts must analyze regulations and law and derive policies and requirements to comply with them

2. Ambiguity, cross-references and evolution of regulations hinder compliance a systematic derivation of requirements

3. Security, safety, and privacy are important legal requirements for modern, “intelligent” online systems

4. Purpose limitation, data minimization, transparency, and data security are legal principles to protect user privacy