Privacy

Computer Security
1DV700

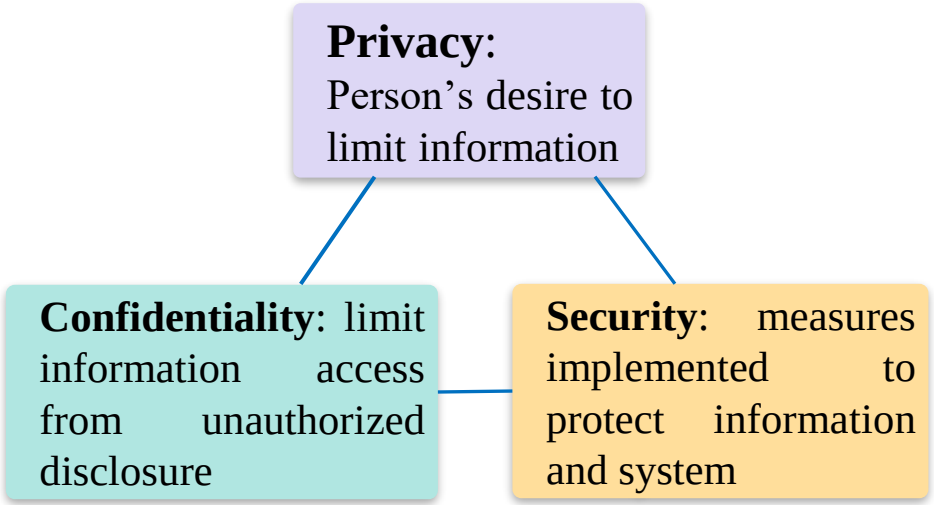
Faiz Ul Muram, Ola Flygty
Linnaeus University, Sweden
{faiz.ulmuram, ola.flygty}@lnu.se

Objectives and Contents

Privacy Definition and Problems	Privacy Principles and Laws	Privacy in Common Criteria
The Information Lifecycle	Web Surfing: Cookies, Spyware, Email	Privacy Concerns in Emerging Technologies

Privacy and Data Protection

- Privacy: the **claim** of individuals, groups and organizations to determine for themselves, **how, when** and to **what** extent information about them is **communicated** to others [Alan Westin 1967]
- Privacy includes concerns of data collection, transmission, data storage, access and rights, usage and disclosure [Moghe 2003]
- Privacy is part of confidentiality (privacy, secrecy) captures this aspect of computer security
  - Sometimes privacy concerns protection of personal data, while secrecy is used for protection of organizational data



Privacy: Personal Data

- A person's privacy expectations depend on context: who is affected, how that person **feels** about **publicity**, and what the **prevailing norm** of privacy is
- Personally identifiable information (**PII**) is any information that can be used to uniquely **identify**, **contact** or **locate** an individual
- Types of data many people consider private or personal:
  - **Identity**: name, personal number
  - **Financial status**: salaries, tax information
  - **Health**: medical tests, hospital stay
  - **Biometrics**: fingerprints, voice pattern
  - **Location data**: schools, jobs, travel
  - **Legal**: criminal records, marriage

Taken from the internet

Computer-Related Privacy Problems

- **Data Collection**
  - Advances in computer storage, databases make it possible to hold and manipulate huge numbers of records, and those advances continue to evolve
- **Notice and Consent**
  - Notice of collection and consent to allow collection of data are foundations of privacy, but with modern data collection, it is often impossible to know what is being collected, e.g., entry into a website may require an acknowledgment of “terms of use”
- **Control and Ownership of Data**
  - Once a user consents to provide data, the data is out of that user’s control. It may be held indefinitely or shared with other entities

Other Threats to Privacy

- Poor system security, negligence or carelessness
- The government gathers and stores data of citizens, residents, and visitors, such as taxes, homeland security, birth certificates, etc.
- Internet as privacy threat, such as unencrypted e-mail, web surfing, attacks
- Many business entities use personal data for commercial gains,
  - For example, email spam, marketing campaigns and cross selling of products, accepting frequent-buyer cards reduces your privacy

Understanding problems and risks is a first step towards protecting privacy

Need: new laws and regulations, privacy policies and technical solutions

Information Stakeholder Concerns

- **Customers or individual**
  - Concerned with how and why their information is collected, used, disclosed, and retained
  - Want restrict access
- **Companies**
  - Trying to strike a balance between collection and use of information
  - Concerned with reducing privacy risk of poor privacy practices
  - Want to leverage good privacy practices and retain trust of customers
- **Governments**
  - Taking increased action on growing concerns about privacy to:
  - Protect rights of citizens, residents and better manage its own data stores
  - Authentication, data access risks

Main Actors and Roles

- Main actors responsible for the data processing:
  - **Data subject:** identified or identifiable person about whom we hold personal data (aka principal)
  - **Controller** is the main responsible party and defined through their ability to define **why** (purpose), **how** (means) data is processed
  - **Processor** processes personal data under the guidance of a Controller
  - There is also a concept of a **Joint Controller** which is essentially two Controllers mutually liable for processing (but it is definitely less common)
  - **Data protection officer** is unique individual that may be internal or contracted for processing of sensitive data or systematic monitoring

The **processor** and **controller** are roles that are tied to **organizations** and are part of the responsibility of existing roles

Privacy Principles

- Ensure that data is stored and processed **lawfully, fairly** and in a **transparent** manner
- **Necessity** and **purpose** of data collection and processing
- Data should be **relevant** to the purpose, adequate, accurate, limited and up to date
- Data subject´s (individuals) **right to information** correction, erasing or blocking of incorrect / illegally stored data
- **Set limits** based on the purposes of the processing and data destroyed if no longer necessary for that purpose
- **Safeguards** against loss, corruption, destruction, or misuse of data should be established
- A data controller should be designated and **accountable** for complying with the measures to effect these principles

Privacy Principles and Laws

- Privacy is a **fundamental human right** that has become one of the most important rights of the modern age
- Increasing impact of European Court of Human Rights (Article 8)
  - "Everyone has the right to respect for his private and family life, his home and his correspondence"
- Different countries have taken **different approaches** to **recognizing** and **assuring** a right to privacy
- The **EU** personal data **concept** covers any **data that is linked**, or can be linked to a **person**. In the **U.S.**, the term is usually **Personally Identifiable Information (PII)**

U.S. Data Privacy Laws

- **Privacy Act** of 1974 embodies most of the privacy principles but applies only to data collected by the U.S. government
  - Privacy laws in the U.S. vary by municipality and state

Other federal privacy laws:

- Health Insurance Portability and Accountability Act (**HIPAA**) 1996
- Federal Trade Commission (FTC) has jurisdiction in 2000 for privacy policy of government websites and e-Government Act was enacted in 2002
- Children's Online Privacy Protection Act (**COPPA**) 1998
- Gramm-Leach-Bliley Act (**GLBA**) was enacted on 1999 to protect consumer financial privacy
- Family Educational Rights and Privacy Act (**FERPA**)

European Union Data Directive

- European Union (EU) Data Directive (1995) on the protection of individuals with regard to the processing of **personal data** and on the **free flow** of data within the EU
  - The requirements apply to government, businesses, and organizations
  - The Directive is organized around the following principles: **notice, consent, consistency, access, security, onward transfer, enforcement**

- EU's 2002 ePrivacy Directive, also referred to as the 'cookies law', sets out rules on electronic communications including emails, phone calls, use of cookies that track website visitors' information, …

- Directives set minimum standards and parameters for the EU but leave the actual implementation down to the states themselves

European Union Data Protection Regulation

- General Data Protection Regulation (**GDPR**) 2018 aimed to blend data privacy laws across Europe
  - to **guard** and **authorize** EU nationals' information privacy
  - to **redesign** the way organisations across the region **interpret** and **address** information **privacy**
- It regulates personal data processing. Processing covers practically anything that one can do to personal data - including storage

https://gdpr.eu/

European Union Regulations

- GDPR applies both to organisations located **within** the EU and **outside** the EU if they **offer goods or services** to EU data subjects
- Non-compliant organisations face penalties – up to 4% of annual global turnover or €20 million
- In January 2017, the European Commission proposed a new **ePR** (Regulation on Privacy and Electronic Communications) as part of its **digital single market** strategy
- https://ec.europa.eu/info/law/law-topic/data-protection_en

Privacy in Common Criteria and Controls

- **Anonymity:** a user can use a resource or service without revealing the his/her identity
  - For example, some people like web anonymity and use other IDs because it reduces fears of discrimination
  - Anonymity have it's own advantages and disadvantages

- **Pseudonymity** or de-identified: unique identifiers or key values can be used to link records in a server's database but that cannot be used to trace back to a real identity
  - For example, usage and charging for phone services without disclosing identity

- **Multiple Identities:** a user may have multiple identities

http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf

Privacy in Common Criteria and Controls

- **Linking:** identities correctly to create dossiers and break anonymity creates privacy risks but linking them incorrectly creates much more serious risks for the use of the data and the privacy of affected people
  - your credit card or car registration numbers are your identity may (or may not) be held in your name

- **Unlinkability:** sender and recipient cannot be identified as communicating with each other
  - Data minimisation: It aims separating different data sets, e.g., if they belong to different purposes or domains

- **Unobservability:** a user may use a resource or service without others (especially third parties), being able to observe that the resource or service is being used

Consequences: Not Protecting Personal Data

- **Sony Pictures Entertainment Hack**
  - On November 2014, confidential information including information about employees, e-mails, salaries etc. were exposed
  - It is believed that this cyberhack has cost Sony Pictures approximately $15 million damage recovery
  - Leak of information has caused chaos between many well-known celebrities, and a high number of court trials have been sentenced

- **Home Depot Data Breach**
  - On September 2014, hackers attack on a payment system which resulted in 53 million stolen customer e-mails and 56 million customer credit card accounts
  - It is believed that this incident has cost the company $34 million to overcome this situation

ISO 29100, How Can Organizations Secure Its Privacy Network? https://pecb.com/whitepaper/iso-29100--how-can-organizations-secure-its-privacy-network

Organizational Response

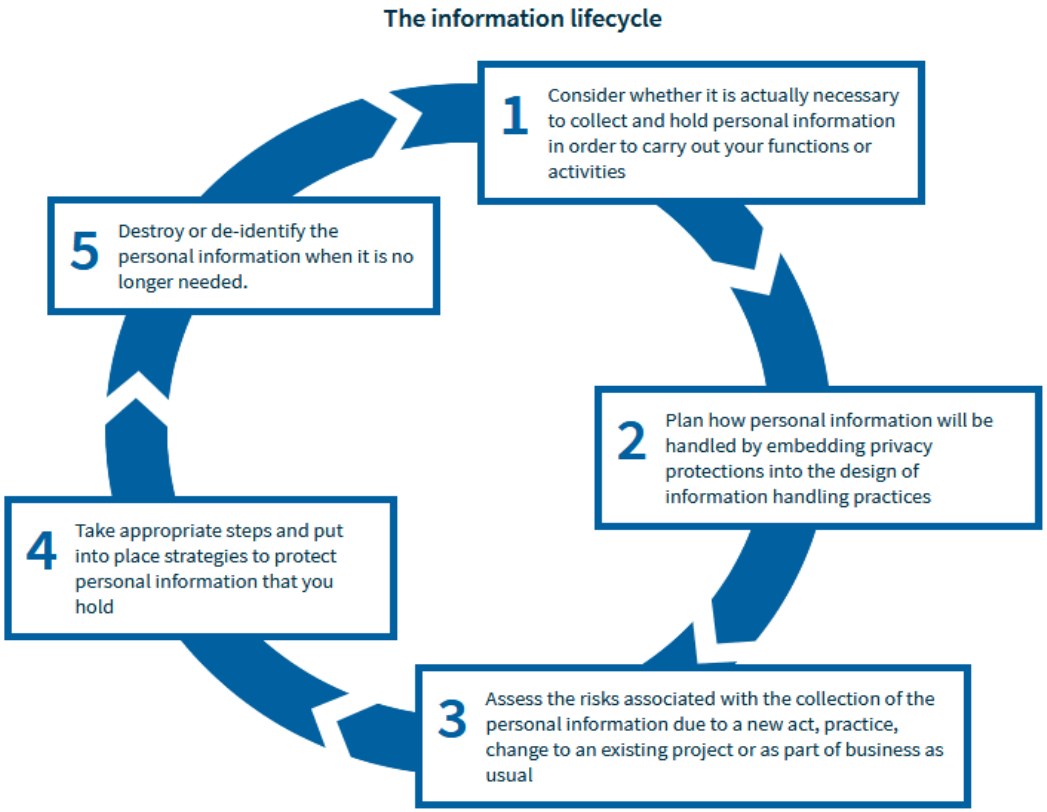
- An organization's data **policy for privacy** and **protection** of identifiable information should be developed and implemented
- The management controls and technical measures should **comply** with all **relevant laws and regulations** concerning privacy as well as to **implement policies** concerning privacy
- Privacy officer, who should provide guidance to managers, users and service providers on their roles and **responsibilities**
  - The specific **procedures** that should be **followed**
  - Ensuring awareness of the privacy principles
  - Reduce the number of security breaches

Policy: What is/what is not allowed, a high-level document

Procedure: How you enforce policy

The Information Life Cycle

- Standards provide guidelines for organizations in addressing privacy issues within their own environment
- Office of the Australian Information Commissioner (OAIC) provides guideline for securing personal information



Taken from https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information

Mapping of ISO/IEC 27000 Standards with GDPR

- **ISO/IEC 27001:** ISMS (information security management system).
- **ISO/IEC 27002** on code of practice for information security controls (and indirectly ISO/IEC 27001 Annex A)
- **ISO/IEC 27005** on risk management

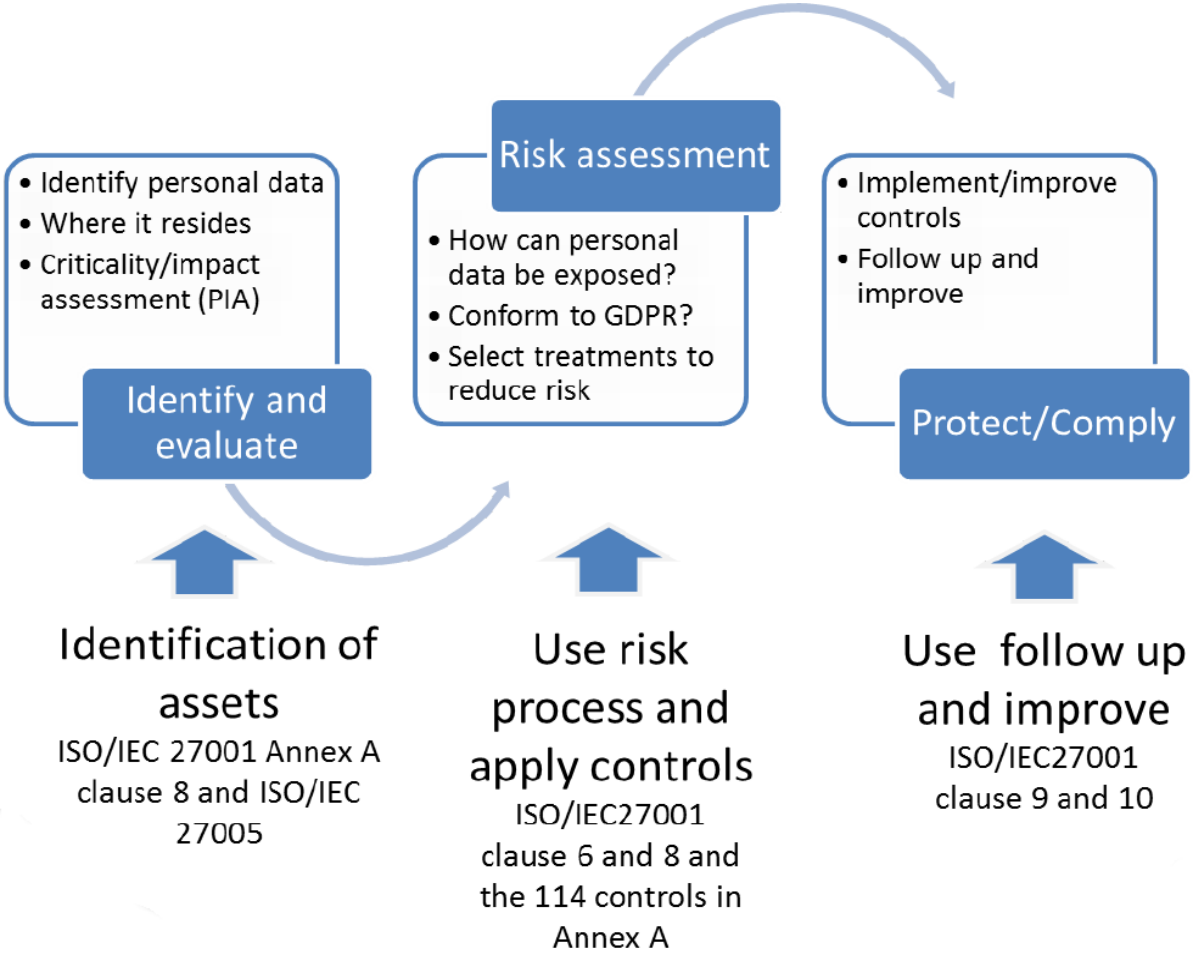


Figure taken from https://dfs.se/wp-content/uploads/2019/05/ISMS-and-GDPR_EN_v1.2.1.pdf

Risk Assessment

- Personal information security risks can be assess by conducting
  - Privacy impact assessment (PIA)
  - Information security risk assessment and
  - Regular reviews of your personal information security controls

Privacy Impact Assessments (PIA)

- PIA assesses the potential future impacts on privacy of a process, information system, programme, software module, device, etc.
  - Privacy impact is the result of personal data processing, data breaches or data collection
- Considering privacy issues at the early stages of a project cycle will reduce potential adverse impacts on privacy
- Define recommendations for managing, minimising or eliminating those impacts
- GDPR specifies a special type of PIA called Data Protection Impact Assessment, or DPIA
- PIA report may include documentation about measures taken for risk treatment or evidence relating to compliance with privacy related regulations

Four Core Component of the PIA Process

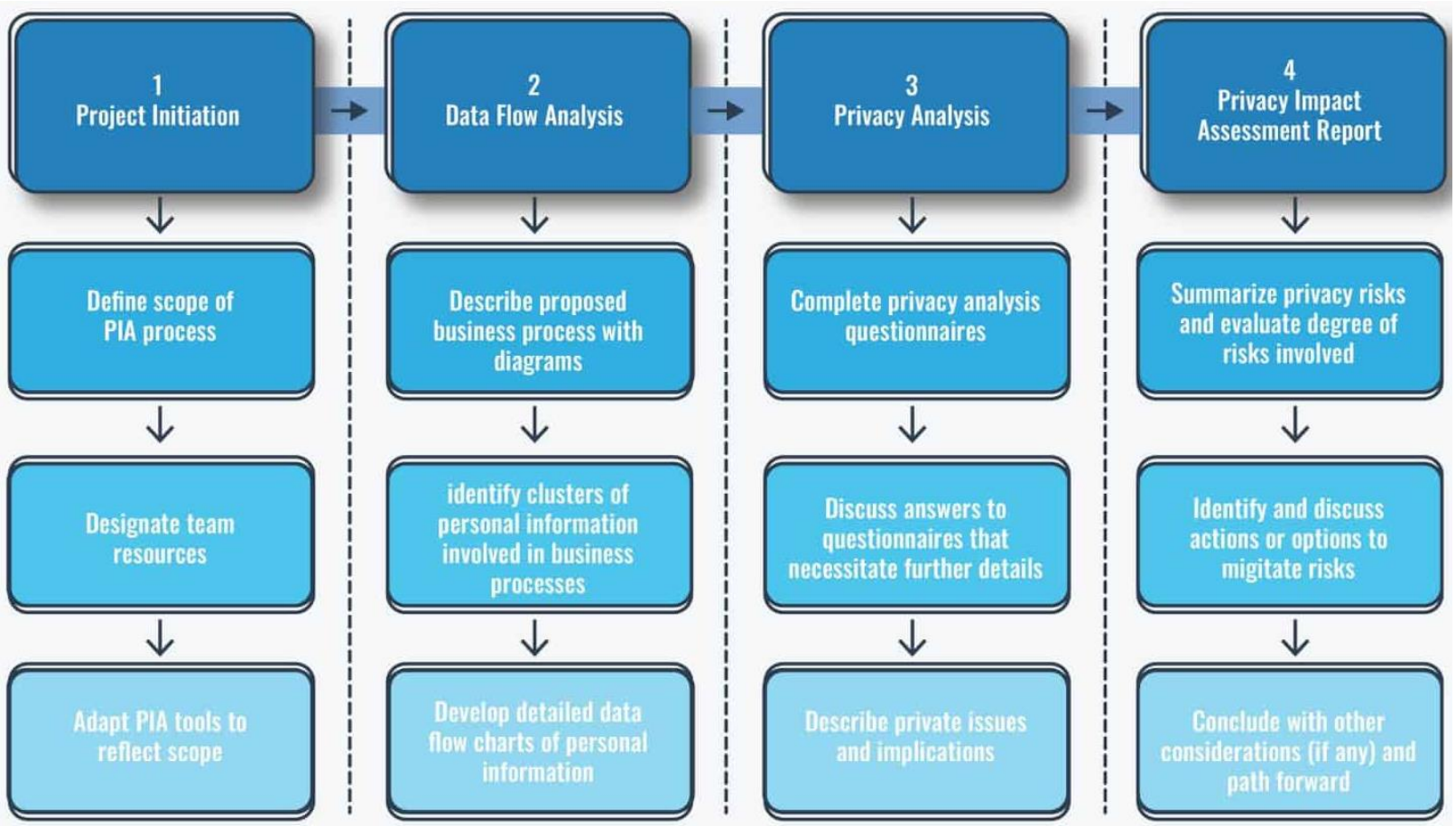


Figure taken from https://www.comparitech.com/data-privacy-management/what-is-a-privacy-impact-assessment/

Information Security Risk Assessments

- It is also known as a **threat risk assessment**, can be conducted in **conjunction** with a **PIA**
- It involves the identification and evaluation of security risks, including
  - threats and vulnerabilities
  - potential impacts of these risks to information handled by an entity

Risk of Human Error

- Threats to personal information can be internal or external as well as malicious or unintentional
- Privacy breaches can arise as a result of human activity or events such as natural disasters
- Apply security controls ISO/IEC 27002

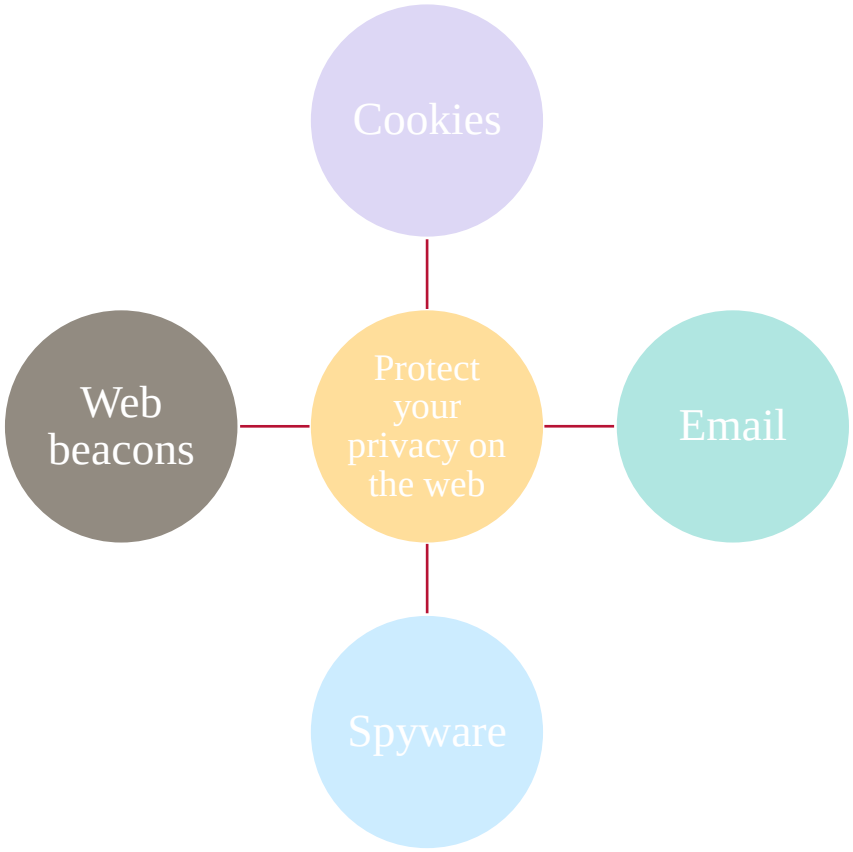
Privacy by Design

- Incorporate privacy into your business planning, staff training, priorities, project objectives and design processes
- Design your personal information security measures with the aim to:
  - prevent the misuse, unauthorised accessing, interference, and modification or disclosure of personal information
  - detect privacy breaches promptly
  - be ready to respond to potential privacy breaches in a timely and appropriate manner
- Select the appropriate technology and measures
- Anticipates and prevents privacy invasive events before they happen

https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

Web Surfing

- Internet technologies keep track of your information
- Internet Service Providers (ISP) always know your IP address and the IP address to which you are communicating
- ISPs are capable of observing unencrypted data passing between you and the Internet



Cookies

- **Cookies** are a way for websites to **store** data **locally** on a user's computer
  - They may contain sensitive personal information, such as viewing preferences, session on website, online shopping, credit card numbers
- **Third-party tracking cookies**
  - Link information from a user's visit to websites of different organizations
  - This tracking information is used for online profiling, which is generally used for targeted advertising
- **Measures**
  - Set up the browser to refuse cookies or warn before storing
  - Opt out targeted advertising by enabling opt out of ads personalisation, delete cookies
  - Software available to manage cookies

Flash Cookies

- **Flash cookies** activated through a **feature** in Adobe's Flash plug-in called Local Shared Objects (LSOs)
- Even if a user has cleared cookie settings (by directing browser to block or delete cookies), sites can still use a feature of Flash to track online behaviour
- Flash cookies are used to ensure smooth playback on sites that stream music and video
- **Measures**
  - Delete all Flash LSOs at the end of each browser session
  - A user must visit Adobe’s site for the deletion controls or use other software

Web Beacons

- Web beacons or web **bugs invisible** (tiny) **graphics** embedded in an image that resides on a web page (email), it can include music or video, has third-party cookie
- Web bug is a privacy threat that has the ability to **immediately** send user behaviour to **advertising services**
- It contains an **executable script** that can perform any action the invoking user permits, such as sending interesting items offsite
- Can be difficult to tell when this action is beneficial and when it isn’t
- Different tools are available for detecting web bug: Bugnosis, Web Bug Detector, Foxbeacom

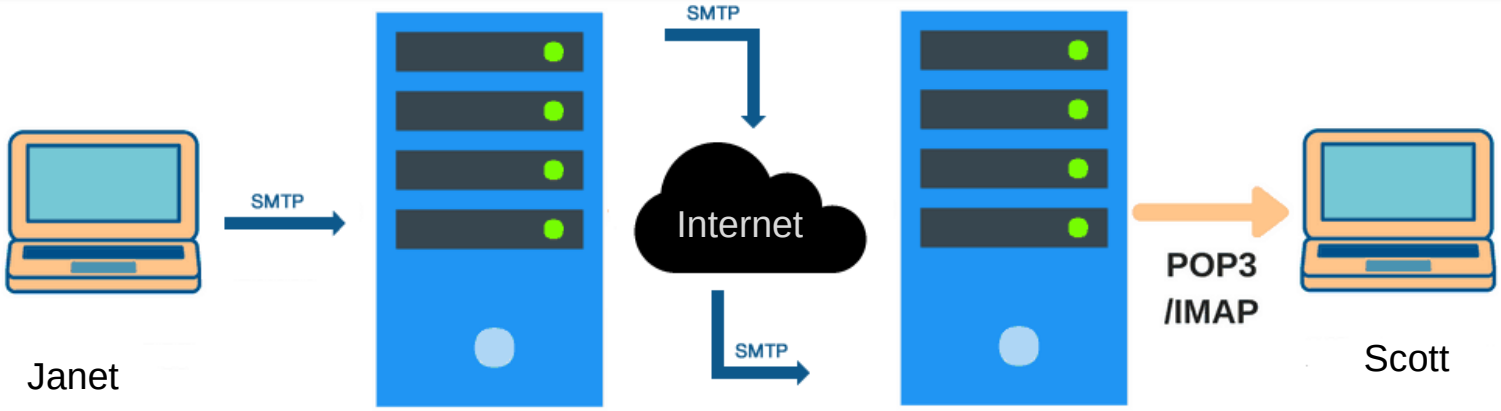
Spyware

- **Spyware** is code designed to track your online movements, **mines** the information stored on your computer, or uses your computer for some tasks without your knowledge
- Often installed in a misleading way as part of other software packages that user has downloaded or exploitation of software vulnerabilities
  - **General spyware:** Advertising applications, identity theft
  - **Hijackers:** Hijack existing programs and use them for different purposes
  - **Adware:** Displays selected advertisements in pop-up windows or the main browser window

- Stability issues, such as application freezing, failure to boot, and system-wide crashes
- **Recommendation**
  - Anti-spyware software for the detection and removal of spyware

Email

- Janet's computer establishes a virtual connection with Scott, and the message is transferred by SMTP (simple mail transfer protocol)
- Scott may not be online, so the message to Scott is stored on a server POP (post office protocol server)
- The message is the transferred through multiple Internet Service Providers (ISPs) and servers before it arrives at Scott's POP
- Any of the servers in this chain of communication can see and keep Janet's email



Email Monitoring

- Most people don’t worry about email privacy on the web due to illusion of anonymity
- Each e-mail you send results in at least 3 or 4 copies being stored on different computers
- Monitoring:
  - Companies and government agencies can legitimately monitor their employees' e-mail use
  - Schools and libraries can monitor the computer use of patrons
  - Network administrators and ISPs can monitor traffic for normal business purposes, such as to measure traffic patterns or to detect spam
  - Organizations usually must advise users of this monitoring, but the notice can be a small sidebar in a personnel handbook or the fine print of a service contract
  - Network users should have no expectation of privacy in their email or general computer use

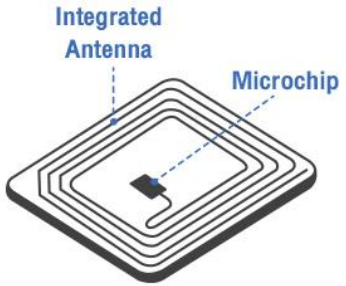
Email Monitoring

- **Email Monitoring in Sweden**
  - A company can check an employee email only if there is a clear description in the terms of use for this and there is a serious suspicion about misuse from the employee
  - Technical monitoring to make sure that the system is working correctly and for instance filtering for spam/virus is ok

- **Phishing** is a form of spam in which the sender attempts to convince the receiver to reveal personal data, such as banking details
- **Help eliminate junk e-mail**
  - Do not complete a member profile with online service
  - Do not fill in registration forms unless the purveyor promises not to sell or exchange your information
  - Never respond to spamming, download a spam buster
  - Protect your passwords, make them complicate
- **Use filter software**
  - States are beginning to provide laws banning unsolicited junk e-mail
- **Remailers** are trusted third parties that replace real addresses with pseudonymous ones to protect identities in correspondence

Emerging Technologies

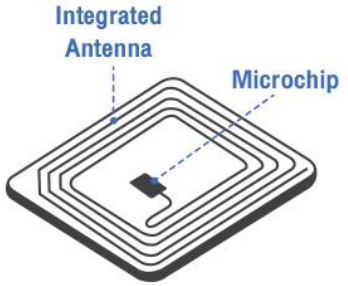
- Impact on Emerging Technologies Privacy in Computing
  - Radio Frequency Identification (RFID) for tracking people
  - Electronic Voting to facilitate elections
  - Voice over Internet Protocols (VoIP) for Voice Grade telephone calls
  - Cloud Computing



Images are taken from the internet

Radio Frequency Identification (RFID)

- RFID tags are small, low-power wireless radio transmitters
- Tags are tuned to a particular frequency and each has a unique ID number
- When a tag receives its signal on the correct frequency, it sends its ID number in response
- Most of these devices are passive until they receive a signal from an interrogating reader
  - Clothing manufacturers sew RFID into cloth. That include garment characteristics, cloth batch etc. for recalls and quality control
  - Stores and malls install readers to limit pilfering and for inventory management
  - Passports and identity cards, can be surgically implanted under the skin of humans or animals



RFID: Security and Privacy Issues

- As RFID tags become cheaper and more ubiquitous, and RFID readers are installed in more places, it may become possible to track individuals wherever they go
- As RFID tags are put on more items, it will become increasingly possible to discern personal information by reading those tags
- Mall owners use the information to dynamically change the advertisements they project on billboards in the Mall
- Correctness: The reading sensor may malfunction or the software processing IDs may fail
- Prediction: Forgery of an RFID tag

Electronic voting

- Electronic voting includes privacy concerns, such as maintaining privacy of who has voted and who each person voted for
- Other issues: tampering of data and availability of voting system

Voice over IP (VoIP)

- While VoIP adds the possibility of encryption to voice calls, it also allows a new set of service providers to track sources and destinations of those calls

Cloud computing

- Physical location of information in the cloud may have significant effects on privacy and confidentiality protections
- Cloud data may have more than one legal location at a time
- Laws could oblige cloud providers to examine user data for evidence of criminal activity
- Legal uncertainties make it difficult to assess the status of cloud data

References

- C. Pfleeger, S. Pfleeger, J. Margulies (2015), *Security in Computing, Chapter 9, Fifth Edition*, ISBN: 9780134085043, Pearson Education
- Alan F. Wes 1967. *Privacy and Freedom*
- Moghe, V. 2003. "*Privacy Management–a New Era in the Australian Business Environment,*" Information Management & Computer Security (11:2), pp. 60-66
- OAIC, Guide to securing personal information 'Reasonable steps' to protect personal information, 2018 https://web.archive.org.au/awa/20190509031938mp_/https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-securing-personal-information.pdf
- Lecture by Prof. Bharat Bhargava, Department of Computer Sciences, Purdue University
- Lecture by Antti Vähä-Sipilä
- ISO 29100, How Can Organizations Secure Its Privacy Network? https://pecb.com/whitepaper/iso-29100--how-can-organizations-secure-its-privacy-network

Assignment 2
Program Security

Computer Security
1DV700

Assignment 2: Introduction

- In this assignment you will take the role of a **software security consultant** for a company: *Loco News*, which is a news magazine in a Swedish city
  - The company has lately expanded from being a small local company to now have a national coverage with more resources available
- Groups of 4 students
- Meetings among your group
- Teaching Assistants (TAs) are the representative of Loco News
- Assign one student as project leader
  - The project leader must notify the TAs about who is in the group and their roles
  - Responsible for booking time with representatives (TAs)

Read Documents

- Lab 2 document provides details of Assignment 2
- Loco News – Program security.pdf
  - Provides the background of Loco News (e.g., number of employees, equipment information), and interview of Consultant with the company's CEO
- Top-10-Flaws.pdf
  - Typical flaws made when developing software
- Assignment2_Report_Template.docx
  - Follow it, then export as pdf format and submit it

- As a security information consultant, you will analyze and assess security systems and measures
- Study flaws and suggest applicable solutions to *Loco News*
- Discuss this in the group and what extra information you need to solve the assignment

- Examples of tools that you can use
  - draw.io https://app.diagrams.net/
  - Intelligent Diagramming | Lucidchart
  - https://www.overleaf.com/ or LNU template

Report should include the following topics

- An overview of the software design document (SDD)
- An overview of the software architecture that would be implemented
  - figures/graphs or by making a list of the major software components
- Limitations of the proposed application
- Description of the software that a programmer would have to use, in order to implement the proposed application
- Description of the software mechanisms that would be used in the application
- Description of the security mechanisms that you plan to implement in the application
- Examples of the operation of the application from the user's perspective

Lnu.se