Introduction to Security and Privacy

Edgar Weippl and Sebastian Schrittwieser

Abstract This chapter on *Security and Privacy* builds on two aspects central to digital humanism: (1) self-determination and (2) humans in the center.

Security refers to a system being in a state of protection against potential threats and risks; what this means specifically depends on the so-called security requirements (Bishop, IEEE Security and Privacy, 1(1), 67–69, 2003). Typically, this pertains to protecting data's (1) confidentiality, (2) integrity, and (3) availability. Thus, security mechanisms are designed to prevent unauthorized access, use, disclosure, disruption, modification, or destruction.

Privacy is the individual's fundamental right to determine and limit who has access to their personal information and experiences, ensuring their ability to maintain personal boundaries, confidentiality, and freedom from unauthorized surveillance (Bélanger and Crossler, Privacy in the digital age: A review of information privacy research in information systems. MIS Quarterly, pp. 1017–1041, 2011). Security and privacy are of utmost importance in this increasingly connected world, as they can help protect individuals, companies, and organizations from data breaches, identity theft, and other malicious attacks.

The goals of digital humanism are to shape technologies in accordance with human values and needs, instead of allowing technologies to shape humans. Our task is not only to rein in the downsides of information and communication technologies but to encourage human-centered innovation (Werthner, The Vienna manifesto on digital humanism. In Digital transformation and ethics (pp. 338–357). Ecowin, 2020).

In the following sections, we will analyze security requirements that can compromise these goals and show which security mechanisms can be employed to protect them. Both security and even more privacy are central to digital humanism—also mentioned as one of its principles.

E. Weippl (✉) · S. Schrittwieser
University of Vienna & SBA Research, Vienna, Austria
e-mail: Edgar.Weippl@univie.ac.at; Sebastian.Schrittwieser@univie.ac.at

H. Werthner et al. (eds.), *Introduction to Digital Humanism*,
https://doi.org/10.1007/978-3-031-45304-5_26

1 Introduction

Digital humanism is an ethical framework that seeks to promote the values of human dignity, freedom, and autonomy in developing and using digital technologies. It emphasizes prioritizing human well-being and social responsibility in technology design, implementation, and use.

Digital humanism recognizes that technology is not neutral and can have significant impacts on individuals and society as a whole. The goal is to ensure that technology is developed and used to benefit people and society while respecting their rights and dignity.

Overall, digital humanism seeks to ensure that technology is developed and used in ways that promote human well-being and respect individuals' rights and dignity. It represents a new approach to technology development that prioritizes human values over purely technological or economic considerations.

Security and privacy can provide essential tools to reach such a vision. Many security requirements are implicitly included in the Vienna Manifesto on Digital Humanism. For instance, accountability requires strong authentication—a core concept in information security.

Privacy and security are closely related concepts in information technology but have distinct meanings and objectives. **Privacy** refers to determining, preserving, and managing the rights and restrictions associated with personal data, ensuring that it is only collected, stored, used, and shared in a manner that respects individual rights and needs and further complies with applicable laws and regulations. In essence, privacy is about ensuring individuals' rights to control their personal information within the digital realm, i.e., that individuals can make informed decisions about how their data is used (Schwartz, 2019).

On the other hand, security is concerned with protecting information systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves implementing technical, physical, and administrative controls to safeguard the integrity, confidentiality, and availability of information. Security measures include firewalls, encryption, authentication, access control, intrusion detection systems, and regular software updates.

While privacy and security are different concepts, they are closely intertwined. A robust **security framework is necessary to protect the privacy** of individuals and organizations by preventing unauthorized access to their sensitive data. Conversely, strong privacy policies and practices can help enhance the overall security of information systems by minimizing the amount of sensitive data collected, stored, and transmitted.

Ransomware, Industry 4.0, the EU General Data Protection Regulation, mobility, home workplaces, public cloud services, and many other topics have dominated the headlines recently. Given the force of these topics and the often still missing comprehensive security architectures needed to master them, it is becoming increasingly common to lose a sense of how these security fields are interwoven and especially how they need to be linked with classic security requirements such as asset management or privacy concepts. Old knowledge meets completely new threats. In companies, it is the task of the IT security manager to maintain an overview and respond to essential threats with the necessary measures in an appropriate manner.

> There are advantages to computerizing everything—some that we can see today, and some that we'll realize only once these computers have reached critical mass. The Internet of Things will embed itself into our lives at every level, and I don't think we can predict the emergent properties of this trend. We're reaching a fundamental shift that is due to scale and scope; these differences in degree are causing a difference in kind. Everything is becoming one complex hyper-connected system in which, even if things don't interoperate, they're on the same network and affect each other. (Schneier, 2018)

2 Basic Concepts and Definitions

Historically, cryptography and "keeping things secret" have been core aspects of **security** (Trček et al., 2007). The first important step is distinguishing between *security requirements* and *security mechanisms* or *countermeasures*. "Keeping things secret" is a security requirement commonly called confidentiality. Cryptography is one possible security mechanism to implement the requirement of confidentiality. However, ensuring confidentiality alone does not make a system secure. The second step is to comprehensively list the basic security requirements and potential mechanisms for their implementation.

There are three basic security requirements:

1. Confidentiality: Ensuring that sensitive data is only accessible to authorized individuals.
2. Integrity: Protecting data from unauthorized modification or destruction.
3. Availability: Ensuring that data is accessible to authorized individuals when needed.

Confidentiality helps to ensure that sensitive data is only accessible to authorized individuals. This includes protecting data from unauthorized disclosure, meaning only those with the proper permissions can view or access it.

Integrity is the second core concept of information security and is defined as protecting data from unauthorized modification. This includes ensuring that data is not modified in transit or at rest by malicious actors or accidentally. Integrity requires that data is not corrupted or altered in any (unauthorized) way. Integrity is essential to maintain the accuracy and authenticity of data, i.e., to ensure that it is not tampered with or misused.

Availability refers to the ability of authorized individuals to access data and services when needed. It ensures that data is available on demand and not disrupted by malicious, accidental, or natural threats. Complete outages or slowdowns compromise a system's availability.

Countermeasures can be categorized in different ways, such as the *type* of countermeasure or according to its *effect*. There are three basic types of countermeasures: (1) administrative, (2) technical, and (3) physical.

The training handbook for the CISSP (Certified information systems security professional) exam defines the countermeasures or controls as follows:

> Administrative controls are commonly referred to as "soft controls" because they are more management-oriented. Administrative controls include security documentation, risk management, personnel security, and training.
>
> Technical controls (logical controls) are software or hardware components, such as firewalls, IDS, encryption, and identification and authentication mechanisms.
>
> And physical controls are items put into place to protect facilities, personnel, and resources. Physical controls include security guards, locks, fencing, and lighting. (Bragg, 2002)

Countermeasures have different ways of doing what they do. They can prevent, deter, detect, correct, or compensate for the effects of an attack or can be used to recover from an attack.

- *Preventive* countermeasures impede a bad event from happening at all.
- *Deterrent* countermeasures will not wholly prevent an incident in all cases but will reduce the likelihood as it dissuades prospective attackers.
- Once an attack or accidental incident happens, a *detective* countermeasure is needed for the system operator or data owner to actually notice that security requirements have been compromised.
- *Corrective* controls are employed after an incident has been detected to fix the problem.
- If no corrective actions can be taken or the problem is too comprehensive, a *recovery* mechanism, such as a backup, is used to restore the system and data to a previous secure state.
- Another mechanism well known to prevent accounting fraud can also be used to protect data and systems. *Compensating* mechanisms offer a second independent way to compensate for the first mechanism should it fail.

All security mechanisms can be categorized along these two dimensions. For instance, encryption is a *technical* countermeasure that *prevents* unauthorized data disclosure, thus protecting data confidentiality.

A related yet different topic is **privacy**. The NIST defines privacy as "assurance that the confidentiality of, and access to, certain information about an entity is protected." (Powell et al., 2022) or "freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual" (Garfinkel, 2015) or "the right of a party to maintain control over and confidentiality of information about itself" (Oldehoeft, 1992).

2.1 Methods

Once we know which security requirements exist, we can examine how some typical countermeasures are implemented.

People often think of encryption first; even many textbooks start with chapters on encryption. Nonetheless, it is crucial to remember that the most critical first step is to know the requirements—we will elaborate on the process of risk analysis in the following subsection and to understand that even powerful security mechanisms, such as encryption, do not automatically solve all security issues. Encryption can be used incorrectly, giving people a false sense of security.

1. Encryption
2. Authentication
3. Access control
4. Compartmentalization

2.1.1 Encryption

Encryption is the process of encoding a clear-text message into a ciphertext so that an attacker cannot decrypt the ciphertext without knowing the encryption key, even though she knows the algorithm used for encryption. The security of all modern encryption algorithms depends on the secrecy of the encryption/decryption key and not on keeping the algorithm itself secret (Kerckhoff's principle).

Encryption security depends on choosing a good crypto algorithm, but more is needed. The encryption/decryption keys have to be selected wisely, too. The message's confidentiality is compromised if an attacker can guess the key.

Another important aspect is if the sender of a message sends only a few different messages (e.g., if there are only two types of messages sent, "buy the share" or "sell the share"). If the same keys are used without modification, the attacker may not be able to decrypt the message but can observe the ciphertexts. The same cleartext encrypted with identical keys always creates the same ciphertext.

More importantly, even if many different messages are sent, simply observing the traffic patterns (e.g., few vs. many messages or short vs. long messages sent) can leak information to an attacker (Paar & Pelzl, 2009).

2.1.2 Authentication

Authentication is a way to make sure that someone is who they say they are. It is like showing your ID to prove that you are really you, in the same way when a website or app may require to enter a username (i.e., the process of identification) and password (i.e., authentication) to prove the user's identity.

In general terms, authentication is the process of confirming an entity's identity, such as a person, device, or system. It involves using various methods and techniques to verify that the entity is who it claims to be. Only once the identity has been verified can the system check which permissions and privileges to access a particular resource or service can be granted (i.e., authorization).

Authentication can be accomplished through a variety of mechanisms, such as (1) passwords or PINs, (2) biometrics (e.g., fingerprint or facial recognition), or (3) smart cards and digital certificates. Two-factor or multiple-factor authentication may be used, such as requiring proof of at least two of the three methods above.

Authentication is an essential aspect of security, particularly in the digital realm. In addition to being the prerequisite for authorization, authentication can also be used to establish trust between entities. For instance, a digital certificate issued by a trusted certificate authority can be used to authenticate the identity of a website, which helps to establish trust with users who visit the site.

Authentication and identity management are crucial aspects of security and trust, and their importance is only likely to grow as more aspects of our lives move online.

2.1.3 Authorization and Access Control

Authorization and access control are two related concepts that are used to determine what resources or services an entity (such as a person, computer process, or system) is allowed to access.

Authorization is the process of granting or denying access to a particular resource or service based on the permissions assigned to the requesting entity. For instance, if a user wants to access a file on a computer, the operating system will check whether the user has the necessary permissions to access that file. If the user does have the required permissions, they will be authorized to access the file. If not, they will be denied access. More specifically, "access" can refer to certain privileges such as "write access," "read-only access," "deleting," etc. (Sandhu & Samarati, 1994).

2.1.4 Compartmentalization

Another important defense concept is compartmentalization, also referred to as defense-in-depth. This is a security strategy that involves implementing multiple layers of protection to safeguard an organization's information systems, networks, and assets from potential threats. This approach is based on the principle that every single security measure can be compromised and that a multilayered defense can provide a more robust and resilient security posture.

The concept of defense in depth originates from a military strategy where multiple layers of defense are used to slow down an attacker's progress, giving the defenders time to respond and making it more difficult for the attacker to breach the defenses.

In the context of information security, defense in depth involves using a combination of technical, administrative, and physical security measures to protect against various attack vectors. Some key elements of a defense-in-depth strategy include:

- **Access control**: Implementing strong access control mechanisms, such as role-based access control and multifactor authentication, to ensure that only authorized individuals can access sensitive information and resources.
- **Network segmentation**: Dividing the network into smaller segments, each with its own security controls, to limit the potential impact of a security breach and restrict the movement of attackers within the network.
- **Firewalls and intrusion detection/prevention systems (IDS/IPS)**: Deploying firewalls to filter incoming and outgoing network traffic, along with IDS/IPS to monitor for and respond to potential threats in real time.
- **Encryption**: Encrypting sensitive data at rest and in transit to protect it from unauthorized access, tampering, or eavesdropping.
- **Patch management**: Regularly updating software, firmware, and operating systems to fix known security vulnerabilities and reduce the attack surface.
- **Endpoint protection**: Deploying antivirus, anti-malware, and endpoint detection and response (EDR) solutions on devices to protect against threats targeting user devices.
- **Security awareness training**: Educating employees about security best practices, common threats, and how to recognize and respond to potential attacks.
- **Physical security**: Implementing measures such as access control systems, surveillance cameras, and secure storage facilities to protect physical assets and prevent unauthorized access to sensitive areas.
- **Backup and disaster recovery**: Regularly backing up critical data and systems and having a disaster recovery plan in place to restore operations quickly in the event of a security incident or other disruptions.

The defense-in-depth approach aims to minimize the likelihood of a successful attack by increasing the difficulty for attackers to navigate through multiple layers of security and providing multiple opportunities for defenders to detect and respond to potential threats.

The same idea can be used to protect an individual's privacy. This refers to a multilayered approach to safeguard personal information and ensure data privacy. Just as with information security, defense-in-depth for privacy involves implementing a combination of technical, administrative, and organizational measures to minimize privacy risks and prevent unauthorized access, use, or disclosure of sensitive data. Some key elements of a defense-in-depth strategy for privacy protection include:

- **Privacy by design**: Integrating privacy considerations into the design and development of products, services, and systems from the beginning. This includes incorporating privacy-enhancing technologies, minimizing data collection, and ensuring that privacy is a core aspect of the development process (Spiekermann, 2012).
- **Access control**: Implementing strict access controls limits who can access personal data and under what conditions. This can include role-based access control, multifactor authentication, and least privilege principles.

- **Data minimization**: Collecting, processing, and storing only the minimum personal data necessary for the intended purpose. This helps reduce the amount of sensitive data that could be compromised in a breach (Pfitzmann & Hansen, 2010).
- **Anonymization and pseudonymization**: Using techniques such as anonymization (Murthy et al., 2019) or pseudonymization (Neubauer & Heurix, 2011) to de-identify personal data, making it more challenging to link the data back to specific individuals and reducing privacy risks.
- **Data encryption**: Encrypting personal data both at rest and in transit to protect it from unauthorized access and interception.
- **Privacy policies and notices**: Communicating privacy policies and practices to users, including information about data collection, usage, and sharing, as well as their rights and choices regarding their personal data.
- **Privacy impact assessments** (PIAs): Conduct regular PIAs to identify and address potential privacy risks and ensure that privacy controls are adequate and up to date.
- **Incident response and breach notification**: Having a well-defined incident response plan in place to address privacy breaches and notify affected individuals and relevant authorities in a timely manner.
- **Employee training and awareness**: Providing regular privacy training for employees to ensure they understand their responsibilities in handling personal data and are aware of privacy risks, policies, and best practices.
- **Third-party management**: Assessing the privacy practices of third-party vendors and partners and ensuring they adhere to your organization's privacy standards.
- **Legal and regulatory compliance**: Ensuring compliance with applicable data protection laws and regulations, such as the GDPR, and staying up to date with changes in privacy legislation.

By implementing a defense-in-depth approach to privacy protection, organizations can build a more robust and resilient privacy posture, reducing the likelihood of privacy breaches and minimizing the potential impact on individuals and the organization itself.

2.2 Risk Management

Technical people might love implementing technical security controls, but it is essential to spend resources efficiently. Therefore, risk management needs to be established as an ongoing task. A good starting point for risk management is performing a risk assessment and then updating this information.

The freely available NIST 800-30 (Ross et al., 2022) guidelines suggest for main steps:

1. Prepare for the assessment.
2. Conduct the assessment:
   (a) Identify threat sources and events.
   (b) Identify vulnerabilities and predisposing conditions.
   (c) Determine the likelihood of occurrence.
   (d) Determine the impact.
   (e) Determine risk.
3. Communicate results.
4. Maintain assessment.

The organization needs to know its assets and security requirements to perform these steps. This is a prerequisite to identifying, for instance, vulnerabilities specific to each asset.

2.2.1 BIA

A business impact analysis (BIA) is a critical step in creating a business continuity plan. It helps identify the potential impacts of a disruption to business operations. It implicitly prioritizes critical business processes and functions that need to be restored first when a disaster recovery plan is executed. However, disaster recovery is only one possible control to implement business continuity. Redundancy, for instance, would be a compensating control.

Performing a BIA is essential as it—as previously stated—focuses on the requirements. More precisely, not only on the technical requirement of confidentiality, integrity, and availability but instead applies them to specific (information) assets.

The usual steps in a BIA are:

- **Define the scope**: Identify the areas included in the BIA. For companies or institutions, this may include facilities, departments, business processes, and technology systems. For private individuals, this included listing the areas of life which use IT or depend on such infrastructure such as personal photos, documents, travel arrangements, tax records, letters/documents, and communication with banks, insurance companies, etc.
- **Identify the critical (business) functions**: List all of the critical (business) functions and prioritize them based on their importance. This can be done by identifying the functions that would have the most severe impact if disrupted. When elaborating on the disruption, the three basic security requirements (CIA) are essential to consider. For instance, the confidentiality of your vacation photos might not be as crucial as the general availability regarding recoverability. While you can most likely accept not having access to them for a couple of days or weeks, completely losing them would be a big (personal) loss.
- **Identify the dependencies**: Identify the dependencies between the critical business functions and other departments, systems, vendors, and partners. This will help you understand how a disruption in one area could impact others. In

particular, if you are using cloud services to store your data, think about the impact of the provider's failure. As commonly mentioned tongue-in-cheek, the cloud is simply "someone else's computer."

The next step is a risk analysis to analyze how frequently a bad event might happen and how bad it is expected to be. Based on these findings, one can look at possible controls and then decide on the cost-effective ones to be implemented.

- **Determine the impact and likelihood**: Determine the potential impact of a disruption to each critical business function. This includes the financial, operational, and reputational impacts that arise if confidentiality, integrity, or availability is compromised.
- **Define recovery time objectives**: Determine the maximum time each critical business function can be down before it starts to impact the organization significantly. This will help prioritize which functions must be restored first should recovery controls be implemented.
- **Analyze controls**: Analyze which controls can be used to protect each critical business function, for instance, using the two aforementioned dimensions: (1) *type* of countermeasure and (2) its *effect*.
- **Test and update the plan**: Test the plan regularly to ensure that it works and update it as necessary to reflect changes in the organization, the assets, and the services used.

Overall, a BIA is an essential step in ensuring that your organization can recover quickly from disruption and continue to operate in the event of an unexpected event or disaster.

2.2.2 PIA

A privacy impact assessment (PIA) is a structured process that helps organizations identify and address privacy risks associated with new projects or initiatives. This involves assessing the privacy impact of a project or initiative, identifying risks, and developing strategies to mitigate them.

Performing a privacy risk analysis typically involves several steps:

- **Identify the data**: Begin by identifying all the data being collected and processed, including personal information, sensitive data, and any other information that could pose a privacy risk.
- **Identify the risks**: Determine the potential risks that could arise from collecting and processing the data, such as unauthorized access, accidental disclosure, or misuse of data.
- **Evaluate the risks**: Assess the likelihood and impact of each identified risk, considering factors such as the sensitivity of the data, the potential harm to individuals, and the likelihood of a breach occurring.
- **Identify safeguards**: Identify measures that can be taken to mitigate the risks, such as implementing access controls, encryption, or anonymization techniques.

- **Evaluate safeguards**: Evaluate the effectiveness of the safeguards in mitigating the risks, and identify any potential gaps or weaknesses that need to be addressed.
- **Document the analysis**: Document the findings of the privacy risk analysis, including the data and risks identified, the safeguards implemented, and any recommendations for further action.

It is important to note that privacy risk analysis is an ongoing process and should be reviewed and updated regularly to ensure that the organization's data protection measures effectively address new and emerging privacy risks.

1. *Qualitative analysis:* This method involves identifying privacy risks and assessing their likelihood and impact using a qualitative approach. This may involve brainstorming sessions with stakeholders, interviews with subject matter experts, and reviewing past incidents and security assessments.
2. *Quantitative analysis:* This method uses statistical and mathematical methods to measure the likelihood and impact of privacy risks. This may involve gathering data on past incidents and conducting simulations to model potential threats and their impact.

3 Critical Discussion

Digital humanism refers to integrating digital technologies and human values to prioritize human needs, rights, and well-being. While this concept promotes a more people-centric approach to technology, it also brings several privacy challenges. Some of these challenges include:

- **Data collection and surveillance**: The increasing pervasiveness of digital technologies has led to massive data collection, which can be misused for surveillance purposes. This compromises people's privacy and personal freedom, often without their consent or knowledge.
- **Data breaches and leaks**: As data is stored and transmitted digitally, it becomes vulnerable to breaches and leaks. Hackers can exploit vulnerabilities in systems to steal sensitive personal information, posing significant privacy risks for individuals.
- **Inadequate data protection laws**: Many countries need robust data protection laws, or their existing laws may need to be revised to protect privacy in the context of emerging technologies. This leaves individuals exposed to potential privacy violations.
- **Profiling and discrimination**: With the accumulation of personal data, there is a risk of creating profiles based on individuals' behaviors, preferences, and other characteristics. This can lead to employment, housing, or even social interaction discrimination.
- **Loss of anonymity**: The increasing digital footprint makes it difficult for individuals to remain anonymous. Many online platforms and services require

personal information for verification purposes, which can make it difficult for users to maintain their privacy.

- **Consent and control**: Obtaining informed consent from individuals before collecting their data remains challenging. Many users may not fully understand the implications of sharing their data or have no control over how it is used or shared.
- **Algorithmic transparency and bias**: Many digital systems use algorithms to process and analyze data, often in a black-box manner. This lack of transparency can lead to biased outcomes, privacy violations, and unfair treatment.
- **Privacy vs. security trade-offs**: To ensure public safety and national security, governments may prioritize surveillance and data collection, which can infringe on individual privacy.
- **Privacy in the age of the Internet of Things** (IoT): IoT devices can collect vast amounts of data about individuals' habits and preferences, which can pose significant privacy challenges if not managed correctly.

Addressing these challenges requires a concerted effort from policymakers, technology developers, and users to ensure that privacy is protected while allowing digital technologies to flourish and benefit society. However, it is even more challenging as globalization couples previously independent systems of companies providing global services. Privacy expectations vary considerably between countries and political systems, making it hard to know what policies should be implemented:

> There are advantages to computerizing everything—some that we can see today, and some that we'll realize only once these computers have reached critical mass. The Internet of Things will embed itself into our lives at every level, and I don't think we can predict the emergent properties of this trend. We're reaching a fundamental shift that is due to scale and scope; these differences in degree are causing a difference in kind. Everything is becoming one complex hyper-connected system in which, even if things don't interoperate, they're on the same network and affect each other. (Schneier, 2018)

Several global initiatives and frameworks aim to regulate privacy and data protection. These initiatives often serve as models for countries to develop their privacy legislation and policies. Some of the most prominent initiatives and frameworks include the (1) General Data Protection Regulation (GDPR), which continues the development of the Council of Europe Convention 108, (2) OECD Privacy Guidelines, (3) the APEC Privacy Framework, and (4) UN initiatives.

GDPR is a comprehensive data protection law implemented by the European Union (EU) in 2018. It aims to give EU citizens more control over their personal data and harmonize data protection laws across the EU. GDPR has extraterritorial scope, meaning that it also applies to organizations outside the EU that process the personal data of EU citizens. *The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Greenleaf, 2018) is an international treaty that establishes minimum standards for data protection. It has been ratified by many countries, including non-European ones, and has influenced the development of national data protection laws worldwide.

The Organization for Economic Cooperation and Development (OECD) published its **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data** in 1980, updated in 2013.[1] These guidelines provide a set of privacy principles that serve as a foundation for national legislation and international agreements on data protection.

The Asia-Pacific Economic Cooperation **(APEC) Privacy Framework** (APEC, 2005) is a set of privacy principles designed to facilitate the free flow of information while protecting individual privacy rights within the APEC region. The framework provides a foundation for the development of national privacy laws and promotes cross-border data transfers between APEC member economies.

The UN has also contributed to privacy regulation through the International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights (UDHR), which recognize the right to privacy as a fundamental human right. The UN has also released resolutions and reports on privacy in the digital age, such as the report on privacy and ethics in the context of big data (UN Development Group, 2017).

These global initiatives have played a significant role in shaping privacy laws and policies worldwide. They provide guidelines and principles that help countries develop their legal frameworks to protect individual privacy rights while balancing the need for data-driven innovation and economic growth.

4 Simple To-Dos for Users and Companies

As an end user, there are several things you can do to improve security and privacy in any digital system. Here are some of the most important ones:

1. *Use strong and unique passwords*: This is the first line of defense against unauthorized access to your accounts. Use strong and unique passwords for each account, and consider using a password manager to help you generate and manage them.
2. *Keep your software up to date*: Software updates often contain security patches and bug fixes that help protect you against known vulnerabilities. Keep your operating system, web browser, and other software up to date.
3. *Be cautious with links and downloads*: Be wary of clicking on links or downloading attachments from unknown sources, as these could be phishing attempts or contain malware. Always verify the source of the link or attachment before clicking on it.
4. *Use two-factor authentication*: Two-factor authentication adds an extra layer of security to your accounts by requiring a second factor, such as a code sent to your phone, and your password. Enable two-factor authentication wherever possible.

[1] https://www.oecd.org/general/data-protection.htm

5. *Limit the amount of personal information you share*: Be mindful of the personal information you share online, and avoid sharing sensitive information such as your home address, phone number, or social security number.
6. *Review privacy policies and settings*: Take the time to review the privacy policies and settings for the apps and services you use. Ensure you understand how your data is being collected, used, and shared, and adjust the settings as needed to limit the amount of data being collected.
7. *Educate yourself on digital literacy*: Educate yourself on digital literacy to better understand how technology works and the potential risks and benefits it can have. This includes learning about how to protect your privacy and security online, as well as how to identify and respond to phishing and other online scams.

By following these steps, you can help protect your privacy and security online and contribute to a more secure and ethical digital world.

As a company, there are several steps you can take to improve privacy and security in the context of digital humanism. Here are some important ones:

1. *Conduct regular security assessments:* Conduct regular security assessments to identify potential vulnerabilities and ensure that your systems and data are secure. This includes conducting regular penetration testing and vulnerability scans to identify potential weaknesses.
2. *Implement strong access controls*: Implement strong access controls to limit access to sensitive data and systems to only those who need it. This includes implementing multifactor authentication, role-based access controls, and monitoring access logs for suspicious activity.
3. *Use encryption*: Use encryption to protect sensitive data both in transit and at rest. This includes using strong encryption algorithms and protocols to protect data in transit and at rest.
4. *Develop clear privacy policies*: Develop clear privacy policies that outline how you collect, use, and share data, and ensure that these policies are easily accessible and understandable by your users.
5. *Minimize data collection*: Minimize the amount of data you collect to only what is necessary for your business purposes, and dispose of data in a secure and timely manner when it is no longer needed.
6. *Educate employees*: Educate your employees on the importance of privacy and security, and provide training on best practices for protecting data and systems. This includes training on identifying and responding to phishing and other social engineering attacks.
7. *Foster a culture of ethical technology use*: Foster a culture of ethical technology use by ensuring that your products and services align with your company's values and contribute to the public good. This includes considering the potential impacts of your technology on society and the environment and developing technology that is accessible, inclusive, and equitable.

By taking these steps, you can help ensure that your company is contributing to a more secure and ethical digital world.

5 Conclusions

Digital humanism is an ethical framework that emphasizes the importance of human-centered design and values in the development and use of digital technologies. In this context, privacy and security are two critical aspects that must be considered to ensure the protection and well-being of individuals. For an individual, the privacy requirements may—in many cases—be more relevant than security; however, privacy is a fundamental social need of humans, providing a space for autonomy and individual growth and acting as a cornerstone for personal dignity, expression, and freedom from unwarranted scrutiny.

Here are some of the aspects of privacy and security that are important for any digital system and form the basis for an individual's security and privacy in a digital world:

1. **Data protection**: Digital humanism recognizes the value of personal data and the need to protect it from unauthorized access, use, or disclosure. This includes implementing strong data encryption, access controls, and policies that limit the collection and use of personal data.
2. **User control**: Digital humanism emphasizes giving users control over their personal data and how it is used. This includes providing clear and transparent privacy policies, options to opt out of data collection and sharing, and allowing users to delete their data.
3. **Trust** is essential in the development and adoption of digital technologies. This includes ensuring that digital systems are secure, reliable, and transparent and that users have confidence in the technology and the organizations behind it.
4. **Ethical use**: Digital technologies should be used ethically and responsibly. This includes avoiding the use of technologies that could harm individuals or communities, ensuring that technology is used to benefit society, and being transparent about the potential risks and benefits of technology.
5. **Accessibility**: Digital humanism recognizes that technology must be accessible to everyone, regardless of their ability or background. This includes designing technology that is easy to use, providing accessibility features for individuals with disabilities, and ensuring that technology does not discriminate against certain groups of people.

Overall, privacy and security are critical aspects of digital humanism that ensure the development and use of digital technologies align with human values and respect individuals' rights and dignity.

Discussion Questions for Students and Teachers

1. "Digital technologies should be designed to promote democracy and inclusion. This will require special efforts to overcome current inequalities and to use the emancipatory potential of digital technologies to make our societies more inclusive" (one of the core principles in the Vienna Manifesto on Digital Humanism, https://dighum.ec.tuwien.ac.at/wp-content/uploads/2019/07/Vienna_Manifesto_on_Digital_Humanism_EN.pdf).

With digital technologies, many aspects scale much better, also including attacks. Thus, fewer people can do more harm, and attribution is harder. Consequently, one may argue that more surveillance and less freedom are essential to implement the emancipatory potential. What do you think?

2. "Privacy and freedom of speech are essential values for democracy and should be at the center of our activities. Therefore, artifacts such as social media or online platforms need to be altered to better safeguard the free expression of opinion, the dissemination of information, and the protection of privacy" (one of the core principles in the Vienna Manifesto on Digital Humanism, https://dighum.ec.tuwien.ac.at/wp-content/uploads/2019/07/Vienna_Manifesto_on_Digital_Humanism_EN.pdf).

   One of the dangers is the spread of false information and the impression that many people support this view. Given the advances showcased with GPT, AI-based lobbying/influencing bots are a very real scenario. Tying the conversation to one (human) individual may be a remedy. This requires strong authentication and managed identities—centralized as in Europe's eID or also Decentralized IDentifiers (DIDs) as another approach. The drawback is that disallowing anonymous communication is a risk to privacy. Perform a security risk analysis and a privacy risk analysis as a basis for discussion.

3. "Effective regulations, rules and laws, based on a broad public discourse, must be established. They should ensure prediction accuracy, fairness and equality, accountability, and transparency of software programs and algorithms" (one of the core principles in the Vienna Manifesto on Digital Humanism, https://dighum.ec.tuwien.ac.at/wp-content/uploads/2019/07/Vienna_Manifesto_on_Digital_Humanism_EN.pdf).

   Machine learning and data-driven techniques build on the past. Human history is biased, unfair, and unequal. Therefore, making decisions by simply analyzing the past will perpetuate the negative aspects. Changing the future frequently relied on fundamental shifts that one can imagine better as rule-based than based on past data. The concepts of "liberté, egalité, fraternité" did not gradually evolve from Louis XV's reign. Does current information technology lock us in and merely improve efficiency, e.g., AI-based political lobbying, micro-targeting voters, etc., instead of further evolving our society?

Learning Resources for Students

1. B. Schneier, Click Here to Kill Everybody. W.W. Norton, 2018.

   This emphasizes the need to prioritize human safety, well-being, and values in the design and implementation of connected technologies. The book highlights the potential consequences of not addressing security and privacy risks in a hyperconnected world and calls for a holistic approach that places human needs at the center of technology development.

2. "NIST SP 800-30 Rev 1: Guide for Conducting Risk Assessments," NIST, 2012.

   It provides a structured approach to identifying and mitigating risks that may impact human values, privacy, and security in information systems. By conducting thorough risk assessments, organizations and individuals can prioritize and implement measures that protect human needs and well-being in the context of technology usage and development.

3. NIST Cybersecurity Framework—Journey to CSF 2.0 https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

   The framework offers a comprehensive approach to managing and reducing cybersecurity risks that can affect individuals, organizations, and society at large. By promoting better security practices and fostering a culture of continuous improvement, the framework helps ensure that digital technologies are designed and implemented in a manner that respects and prioritizes human values, privacy, and well-being.
4. S. Harris and F. Maymi, CISSP All-in-One Exam Guide. McGraw-Hill, 2021.

   The book helps security professionals develop a comprehensive understanding of information security principles and practices that protect individuals, organizations, and society.
5. OWASP SAMM (Open Worldwide Application Security Project Software Assurance Maturity Model) https://owasp.org/www-project-samm/

   The book provides a framework for organizations to assess, improve, and measure the security of their software development processes. By encouraging the creation of secure software, SAMM promotes a digital environment that respects and protects security and privacy.
6. The Moon is a harsh mistress, Robert Heinlein, G. P. Putnam's Sons 1966.

   The book explores themes of autonomy, freedom, and the role of technology in society. The story, featuring an artificial intelligence that gains self-awareness and assists in a lunar colony's rebellion, encourages discussions about the ethical implications of technology, the responsible development of AI, and the need to consider human values in a technologically driven world.

Acknowledgments SBA Research (SBA-K1) is a COMET Centre within the framework of COMET Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.

References

APE Cooperation. (2005). *APEC privacy framework*. Asia Pacific Economic Cooperation Secretariat, 81.

Bragg, R. (2002). *CISSP training guide: Training guide*. Que Publishing.

Garfinkel, S. L. (2015). *NISTIR 8053. de-identification of personal information*. National Institute of Standards and Technology (NIST).

Greenleaf, G. (2018). "Modernised" Data Protection Convention 108 and the GDPR. In *Data Protection Convention* (Vol. 108, pp. 22–3).

Murthy, S., Bakar, A. A., Rahim, F. A., & Ramli, R. (2019, May). A comparative study of data anonymization techniques. In *2019 IEEE 5th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)* (pp. 306–309). IEEE.

Neubauer, T., & Heurix, J. (2011). A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics, 80*(3), 190–204.

Oldehoeft, A. E. (1992). *Foundations of a security policy for use of the national research and educational network*. US Department of Commerce, National Institute of Standards and Technology.

Paar, C., & Pelzl, J. (2009). *Understanding cryptography: A textbook for students and practitioners*. Springer Science & Business Media.

Pfitzmann, A., & Hansen, M. (2010). *A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management*.

Powell, M., Brule, J., Pease, M., Stouffer, K., Tang, C., Zimmerman, T., Deane, C., Hoyt, J., Raguso, M., Sherule, A. & Zheng, K., (2022). *Protecting information and system integrity in industrial control system environments*.

Ross, R. S., & NIST, S. (2022). *800-30 REV. 1: Guide for conducting risk assessments*. National Institute of Standards and Technology.

Sandhu, R. S., & Samarati, P. (1994). Access control: principle and practice. *IEEE Communications Magazine, 32*(9), 40–48.

Schneier, B. (2018). *Click here to kill everybody: Security and survival in a hyper-connected world*. WW Norton & Company.

Schwartz, P. M. (2019). Global data privacy: The EU way. *NYUL Rev., 94*, 771.

Spiekermann, S. (2012). The challenges of privacy by design. *Communications of the ACM, 55*(7), 38–40.

Trček, D., Trobec, R., Pavešić, N., & Tasič, J. F. (2007). Information systems security and human behaviour. *Behaviour and Information Technology, 26*(2), 113–118.

United Nations Development Group. (2017). *Data privacy, ethics and protection. Guidance note on big data for achievement of the 2030 Agenda*. United Nations.