Tishk International University
Faculty of Applied Science
Cybersecurity Department

Lecture 4: Privacy and Data Protection

CBS221/A : Ethics and Legal Issues in Cybersecurity

Week 4: 26-30/10/2025

Instructor: Prof. Dr. Qaysar Salih Mahdi

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Privacy = right to control personal information.
Ensures data is not misused, leaked, or accessed without consent.
Principle: Information Boundary Theory (Westin, 1967).
Equation: PR = P(D)/S (probability of data breach/safeguards).
Example: Tracking via cookies.
Exercise: Company collects location without consent → Violation of GDPR fairness & consent.
Conclusion: Privacy = fundamental ethical principle.
References: Solove, Understanding Privacy (2008); Solove & Schwartz, Information Privacy Law (2024).

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Introduction to Privacy in Cybersecurity

- **Privacy is how personal data is used and controlled. Privacy focuses on how companies collect, use, and ensure the accuracy of personal information.**
- **When shopping on Amazon, the expectation is that your information will remain confidential. Examples of personal data include mailing and billing addresses, payment information, items purchased, items searched for, and the frequency of purchasing. (Note that none of this information is personally identifiable information (PII) except payment details. Simply put, PII is any information that can verify the identity of a user, such as social security number, birth date, etc.)**
- **Ultimately, Amazon stores data about you that you would most likely want to keep private. Any shopper shares these details with simple expectations. The retailer should:**
- **Keep that information safe.**
- **Not disclose that information to outside parties.**
- **Restrict access to your data to authorized personnel.**
- **The fact that these privacy expectations are largely false—Amazon does sell this information to marketers for a tremendous profit—is a separate topic. However, it is a compelling reason However, it is a compelling reason to thoroughly read the privacy policy of each vendor you do business with online.**

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Information security and information privacy defined

While it may be easy to conflate the two, information privacy is not the same as information security. For information security professionals, the differences between the two concepts are vital. The common understanding of security is more accurately defined as *confidentiality*—or keeping personal information private—when in fact, the practice of information security is much broader.

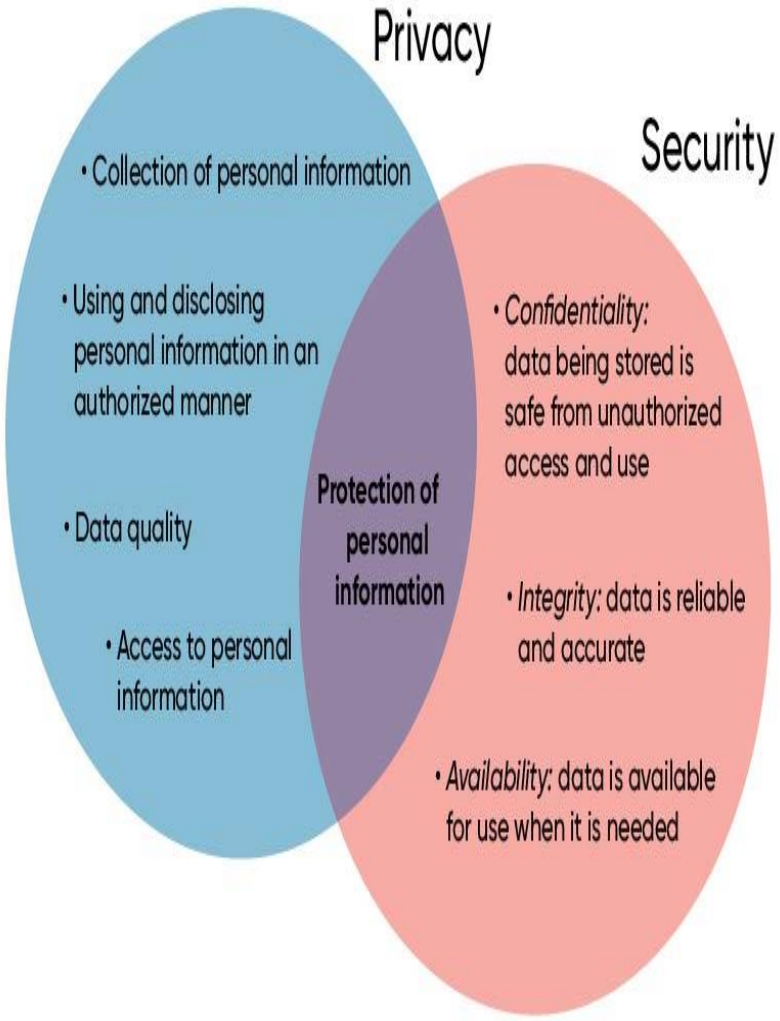
Information security focuses on three concepts, known colloquially as the CIA triad:

- Confidentiality. Stored data is safe from unauthorized access.
- Integrity. Data is reliable and accurate.
- Availability. Data is available on demand.

Information privacy, on the other hand, involves:

- Collection of personal information.
- The authorized usage and disclosure of personal information.
- Data quality.
- Access to personal information.

The overlap between the concepts of information privacy and information security comes from the protection of personal information, which is a crucial concern for both. The differences between information privacy and security are illustrated below.



Tishk International University
Faculty of Applied Science
Cybersecurity Department

Foundations of Data Protection

- Core principles: Confidentiality, Integrity, Availability (CIA).
- Personal vs sensitive data (biometric, health, finance).
- Equation: ISE = f(C, I, A).
- Example: Medical records = sensitive.
- Exercise: Hacker alters medical test → Integrity violated.
- Conclusion: CIA triad as foundation of security.
- t
- Reference: Stallings, Cryptography & Network Security.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Principles of Data Protection

Article 5 of the General Data Protection Regulation (GDPR) sets out key principles which lie at the heart of the general data protection regime. These key principles are set out right at the beginning of the GDPR and they both directly and indirectly influence the other rules and obligations found throughout the legislation. Therefore, compliance with these fundamental principles of data protection is the first step for controllers in ensuring that they fulfil their obligations under the GDPR. The following is a brief overview of the Principles of Data Protection found in article 5 GDPR:

Lawfulness, fairness, and transparency: Any processing of personal data should be lawful and fair. It should be transparent to individuals that personal data concerning them is collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of personal data be easily accessible and easy to understand, and that clear and plain language be used.

Purpose Limitation: Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. However, further processing for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes (in accordance with Article 89(1) GDPR) is not considered to be incompatible with the initial purposes.

Data Minimization: Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum (see also the principle of 'Storage Limitation' below).

Accuracy: Controllers must ensure that personal data are accurate and, where necessary, kept up to date; taking every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. In particular, controllers should accurately record information they collect or receive and the source of that information.

Storage Limitation: Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

Integrity and Confidentiality: Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorized or unlawful access to or use of personal data and the equipment used for the processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Accountability: Finally, the controller is responsible for, and must be able to demonstrate, their compliance with all of the above-named Principles of Data Protection. Controllers must take responsibility for their processing of personal data and how they comply with the GDPR, and be able to demonstrate (through appropriate records and measures) their compliance, in particular to the DPC.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Privacy Rights & Ethical Theories

Rights: autonomy, consent, dignity.

Ethical frameworks: Utilitarianism, Deontology, Virtue ethics.

Example: Social media selling user data.

Problem: Govt mass surveillance.

Solution: Utilitarianism may justify; Deontology rejects.

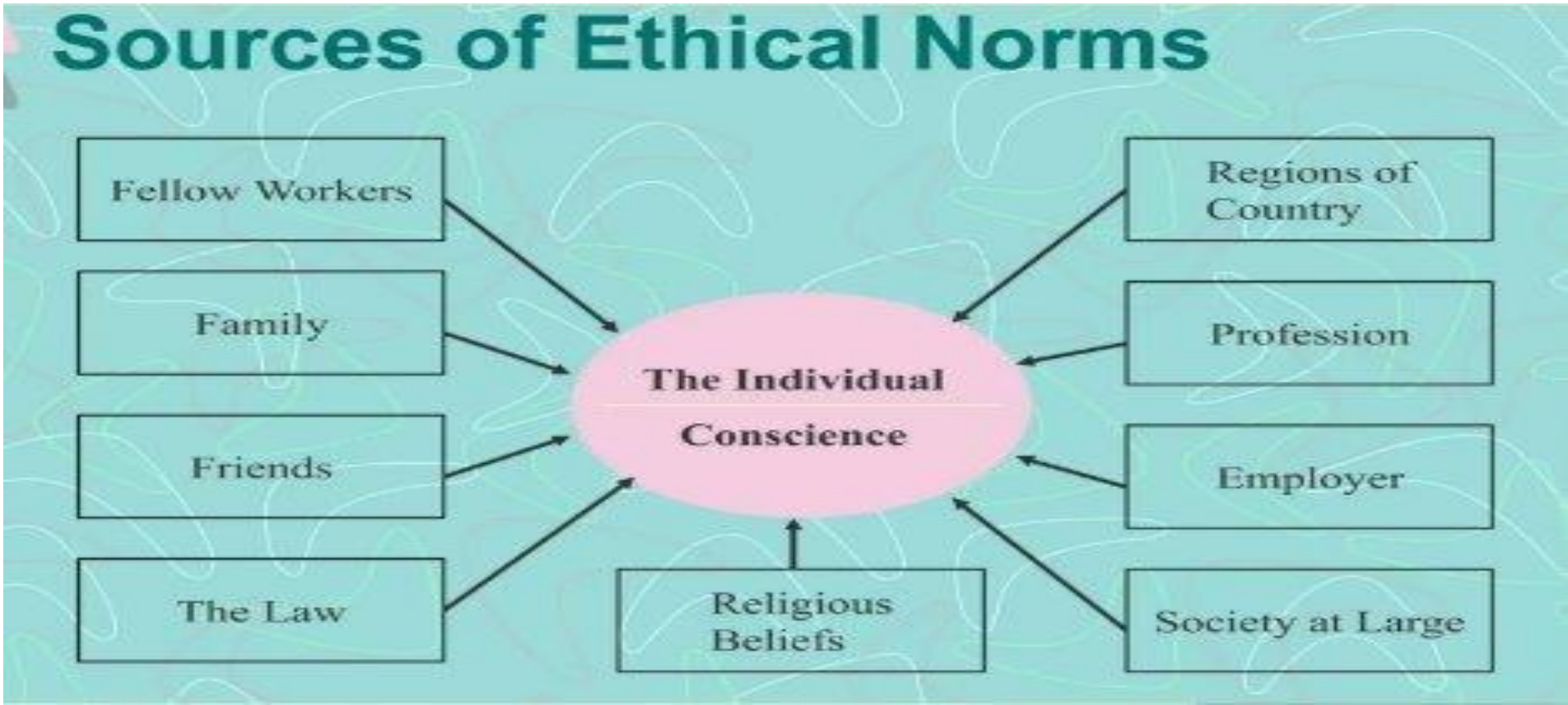
Conclusion: Evaluate privacy dilemmas ethically.

Reference: Quinn, Ethics for the Information Age (2023).

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Ethical Norms

Provide guidance for all organizations for behaving good and keeping away from bad behaviours while promoting ethical behaviours in organization



Tishk International University
Faculty of Applied Science
Cybersecurity Department

3 Types of Normative Ethics

1. **Teleological :** Look at ends or consequences or what we do ?
2. **Deontological** :adheres to independent moral rules or duties ; motives behind certain actions are right or wrong instead of on the rules (Duty-based) 1. Golden Rule 2. Religion (Ten Commandments)
3. **Virtue Ethics** :Virtue ethics is a philosophical approach to morality that centers on a person's character and virtues, rather than focusing on rules or the

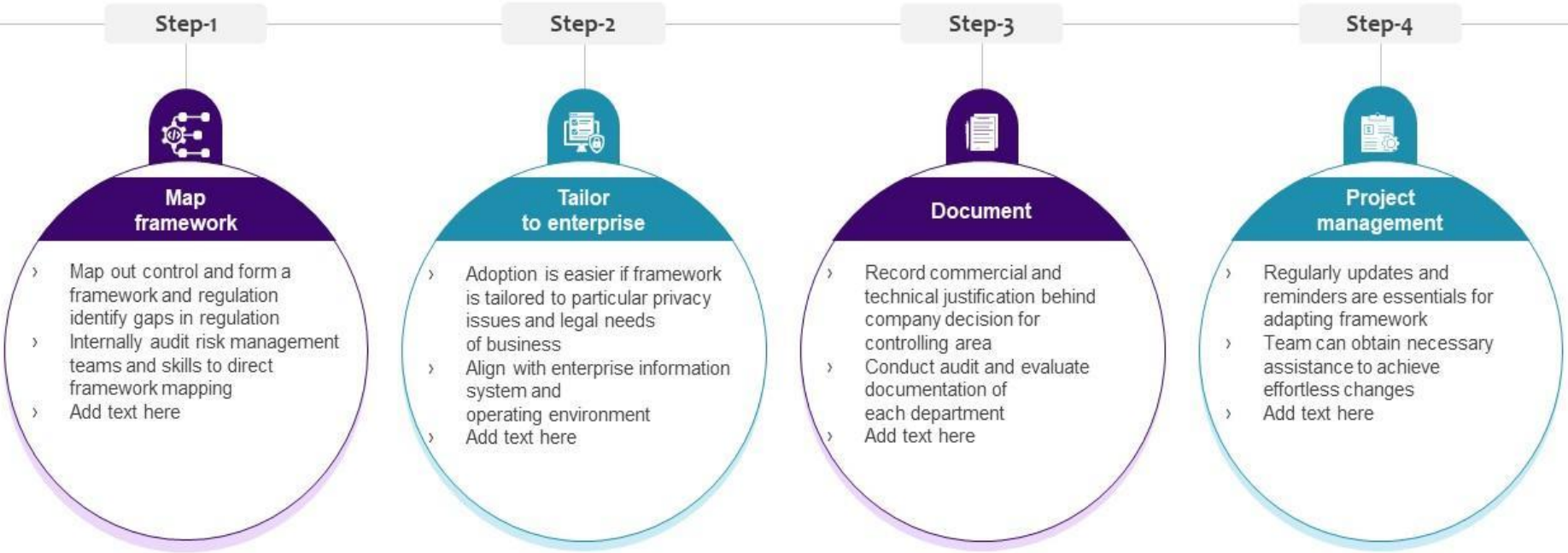
Tishk International University
Faculty of Applied Science
Cybersecurity Department

PERSONAL AND SENSITIVE PERSONAL DATA

Section 30 of the Act defines personal data as "any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual."

4 major implementation steps for privacy framework

This slide showcases key implementation steps for privacy framework. The main purpose of this template is to map out control and form framework and regulation. This includes map framework, tailor enterprise, document, and project management



Tishk International University
Faculty of Applied Science
Cybersecurity Department

Major Privacy Laws & Frameworks

- GDPR (EU), HIPAA (US healthcare), CCPA (California).
- Equation: Compliance Score = Compliant/Total × 100%.
- Exercise: US hospital shares data → HIPAA violation.
- Conclusion: Students know key legal frameworks.
- Image: Reference: Greenleaf, Global Data Privacy Laws (2024).

Tishk International University
Faculty of Applied Science
Cybersecurity Department

GDPR Principles

Principles: lawfulness, fairness, transparency, minimization, accountability.

Exercise: Collecting excessive data → Minimization violated.

Conclusion: Apply GDPR principles to real-world.

Image: https://www.unc-tags.org/data-protection-core-principles

Reference: Voigt & von dem Bussche, EU GDPR (2023).

GDPR Principles

- **Principles: lawfulness, fairness, transparency minimization, accountability.**
- **Exercise: Collecting excessive data → Minimization violated.**
- **Conclusion: Apply GDPR principles to real-world.**
- **Image: https://www.unc-tags.org/data-protection-core-principles**
- https://www.useintegral.com/?gad_source=1&gad_campaignid=20964300440&gclid=EAIaIQobChMIlsyF3subkAMVNaODBx0ykgDaEAAYASAAEgLIbfD_BwE
- **Reference: Voigt & von dem Bussche, EU GDPR (2023).**

Tishk International University
Faculty of Applied Science
Cybersecurity Department

What is the GDPR?

Europe's new data privacy and security law includes hundreds of pages' worth of new requirements for organizations around the world. This GDPR overview will help you understand the law and determine what parts of it apply to you.

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

With the GDPR, Europe is signaling its firm stance on data privacy and security at a time when more people are entrusting their personal data with cloud services and breaches are a daily occurrence. The regulation itself is large, far-reaching, and fairly light on specifics, making GDPR compliance a daunting prospect, particularly for small and medium-sized enterprises (SMEs).

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Consent & Data Collection

- Opt-in vs Opt-out.
- Equation: CVS = f(I, U, R).
- Exercise: Email marketing → explicit opt-in required.
- Conclusion: Consent = cornerstone of privacy.
- Image: https://cdn-icons-png.flaticon.com/512/3135/3135715.png
- Reference: Kuner, Transborder Data Flows (2022).

- Christopher Kuner in his new book Transborder Data Flows and Data Privacy Law aims to bring some clarity into these debates and provide his contribution to the global debate, based on his long experience as one of the most influential data privacy experts e both as a practicing lawyer and as an outstanding academic.
- The book could not be timelier: significant changes to the legal data privacy landscape, business practice and the lives of individuals are brought by many new initiatives and the revisions of the existing international data privacy frameworks, such as the Council of Europe Convention 108, the OECD Guidelines, and the EU Data Protection Directive 95/46.2

Opt-In vs Opt-Out: What's the Difference?

Opt-in and opt-out are key concepts when it comes to complying with online data privacy laws. Many of these laws can either require an opt-in or opt-out approach, so it's important to understand the difference between opt-in vs opt-out and how to implement them.

In short

- Opt-in vs Opt-out
- Opt-in meaning
- Examples of opt-in
- Opt-out meaning
- Examples of opt-out
- What's the difference between opt-in and opt-out?
- When are opt-in and opt-out needed?
- How to implement opt-in and opt-out

Opt-in meaning

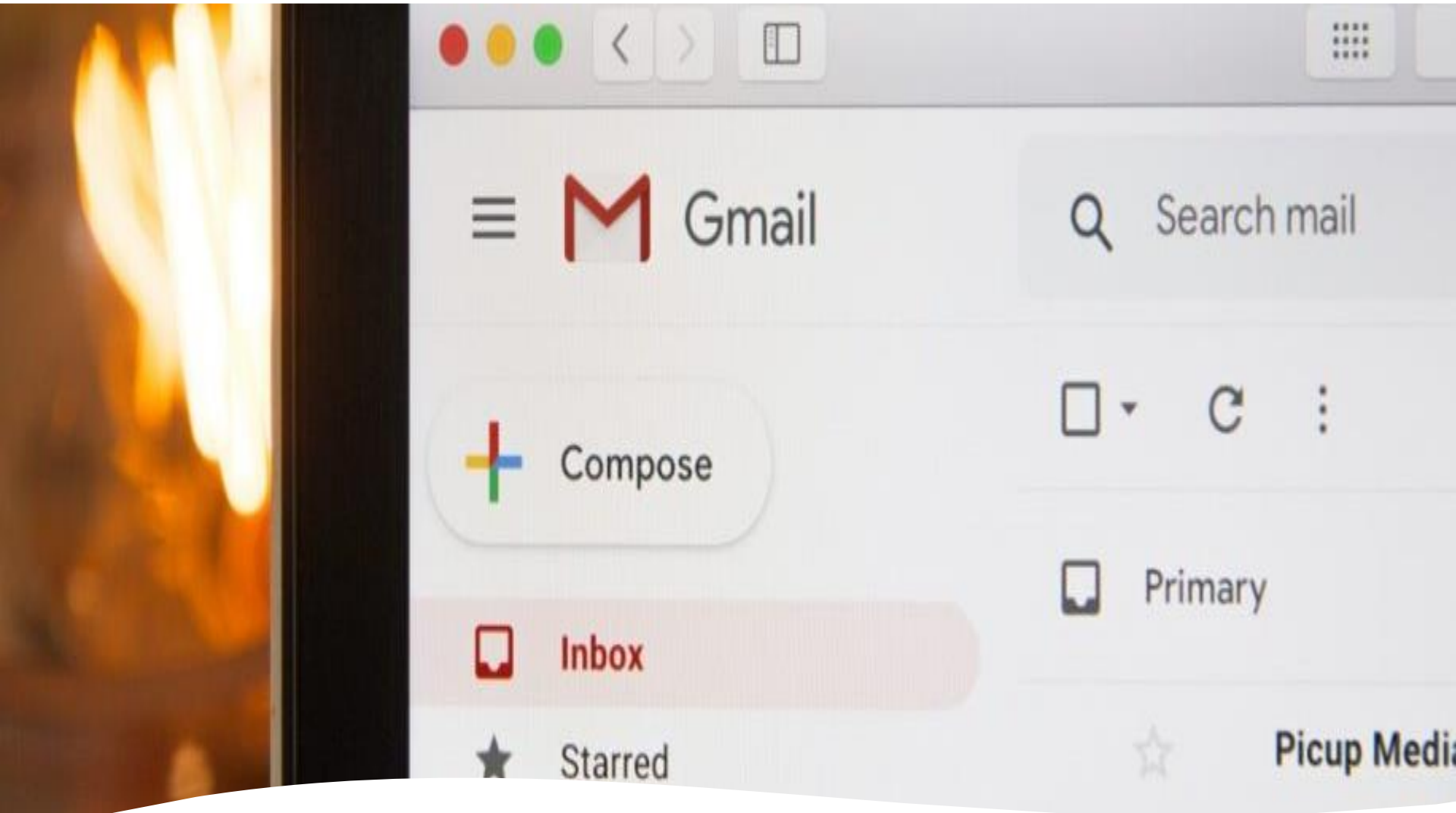
"Opt-in" is the process used to describe when an affirmative action is required to subscribe a user to something, such as a newsletter list. In an opt-in system, explicit action is needed from the user to indicate their willingness to be included.

Examples of opt-in systems are the EU ePrivacy Directive, the General Data Protection Regulation (GDPR), or the Brazilian Lei Geral de Proteção de Dados Pessoais (LGPD).

Examples of opt-in

Let's take the GDPR as a reference. As we said, the GDPR uses an opt-in approach, and – when consent is needed – it must be "*freely given, specific, informed and unambiguous*". That's why the regulation specifically forbids pre-ticked boxes and similar opt-out mechanisms.

Tishk International University
Faculty of Applied Science
Cybersecurity Department



Tishk International University
Faculty of Applied Science
Cybersecurity Department

Newsletter and Marketing Emails

If you have a newsletter or send marketing emails, your users should either enter their email addresses or check a specific box to receive them. Remember not to pre-select the boxes, and have a checkbox for each specific consent you require. For example, you should not combine consent for your Terms and Conditions and your newsletter. You may use two separate boxes.

How to Make your Emails and Newsletter Compliant (with Form Examples)

In Short:

👉 Email and Newsletter Legal Requirements in General

👉 Legal obligations when adding users to your mailing list

- US LAW
- EU LAW

👉 Legal obligations related to Newsletter content

- US LAW
- US LAW

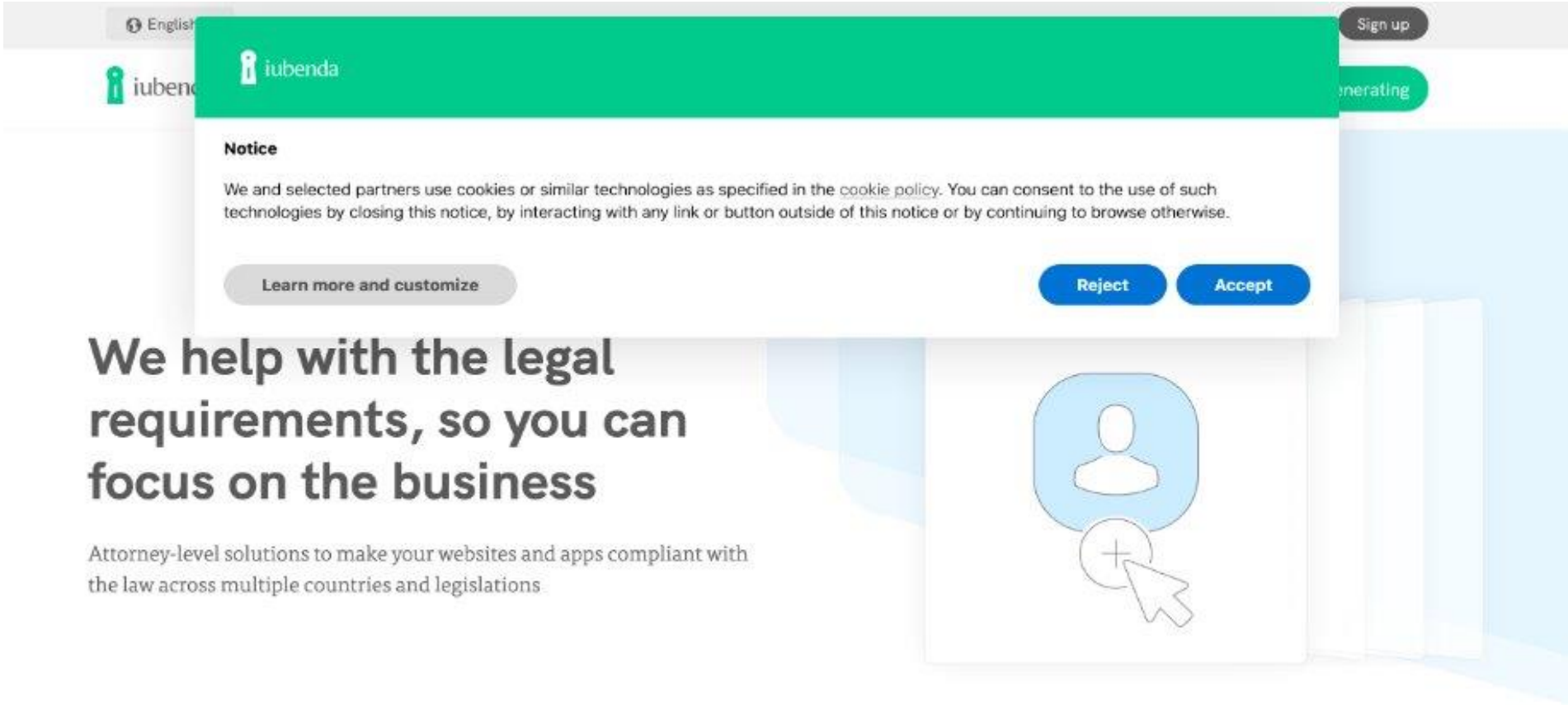
👉 Consequences of non-compliance

✅ Steps for making your newsletter process compliant with the law

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Cookie consent

The EU ePrivacy Directive also requires explicit opt-in consent to install cookies. This is usually done via a cookie consent banner, which is shown on the user's first visit to your website. Without explicit consent, you may only use technical cookies.



Opt-out meaning

On the other hand, opt-out means that a user can be included in something without prior consent, but you need to provide them with an easy way out. So, users can withdraw their consent at any time.

Examples of opt-out systems are the California Consumer Privacy Act (CCPA) and the Swiss Federal Act on Data Protection (FADP), even though there are some exceptions when opt-in consent is required.

Examples of opt-out

Unsubscribe link

One common example of opt-out is the Unsubscribe link you can find at the bottom of newsletters.

Under certain regulations, like the US CAN-Spam Act, you can send your users commercial emails without the need for any action on their part. However, you must always provide them with an Unsubscribe link, so they can easily stop any further communication if they wish to.

The unsubscribe option should be free, not require a login process, and be honored within 10 days.


You are receiving this email because you signed up on our site. Change your email preferences or unsubscribe if you no longer wish to receive emails from us.


Sign up
Email address
Password
Send me information about products, services, deals or recommendations by email (optional)
I accept the sending of advertising material related to relevant third-party products and services, via email (optional)
Create my account


Sign up
Email address
Password
Keep me up to date on exclusive offers by [Company Name] and its partners
Create my account

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Privacy by Design & Default

- Techniques: encryption, anonymization, pseudonymization.
- Example: Apple iOS differential privacy.
- Problem: Linking anonymized data with key = risk.
- Conclusion: Privacy-first system design.
- Image: https://tse1.mm.bing.net/th/id/OIP.4uoVyX0Vw7fAlZSH83kbCAHaFz
- Reference: Cavoukian, Privacy by Design (2011).

Privacy system requirements

- Purpose limitation (comprising both specification of the purpose and limiting the use to that stated purpose)
- Data minimisation
- Data quality
- Transparency (Openness in OECD terms).
- Data subject rights (in terms of consent, and the right to view, erase, and rectify personal data)
- The right to be forgotten.
- Adequate protection (Security Safeguards in OECD terms).
- Data portability
- Data breach notifications.
- Accountability and (provable) compliance

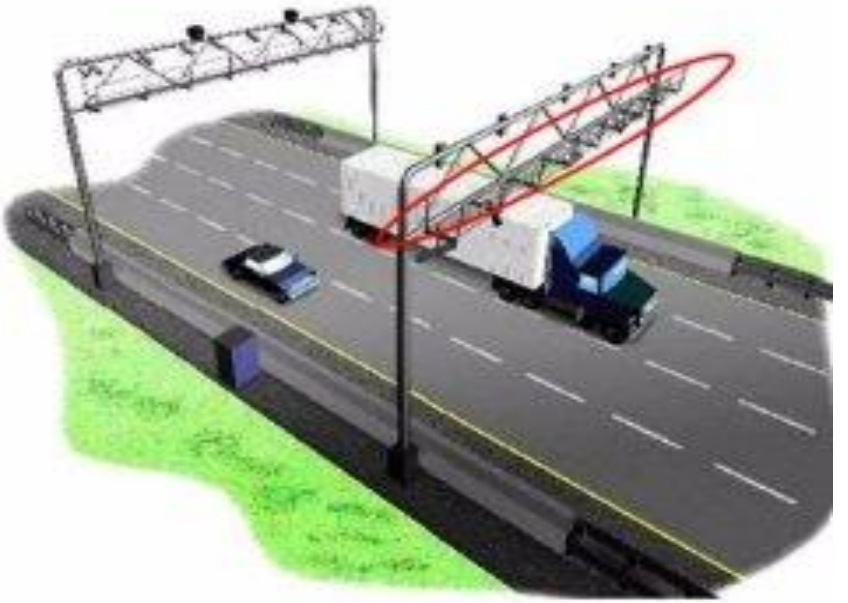
Privacy design strategies

Strategy	Pattern
Minimise	Select before you collect; anonymisation; pseudonymisation
Hide (from all, or third, parties)	Encryption, onion routing, anonymous credentials, homomorphic encryption
Separate	Distributed processing and storage where feasible; split database tables; secure multi-party computation; unlinkability
Aggregate	Aggregation over time and geography; dynamic location granularity
Inform	Transparency, data breach notifications, UI design
Control	Informed consent, UI design
Enforce	Access control, privacy rights management
Demonstrate	Privacy rights management, logging

"Spy bins" and smartphones

Transport pricing

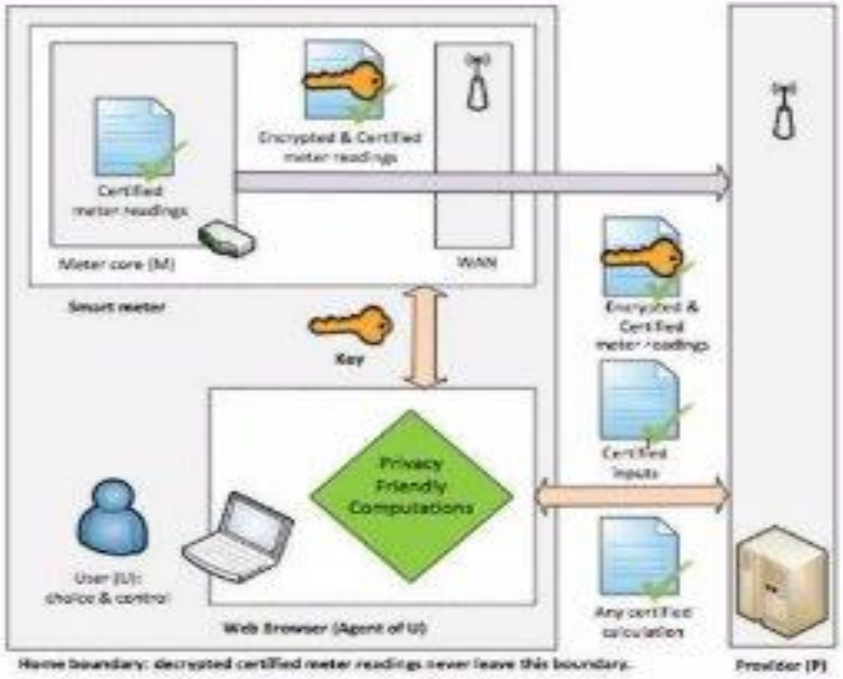
- Monitor all traffic centrally (London), at kerbside (W London) or deduct payment from pay-as-you-go toll cards (Singapore)? On-board unit (Balasch et al. 2010)? Or tax parking spaces?
- Link all payment card usage (Oyster) or use unlinkable RFID tokens (Shenzen)?



MIT Technology Review (2006)

Privacy-friendly smart meters

- Personal data remains at customer premises under their direct control
- Network broadcasts tariff data to meters, which control appliances
- Heavily aggregated information used for billing and price comparison

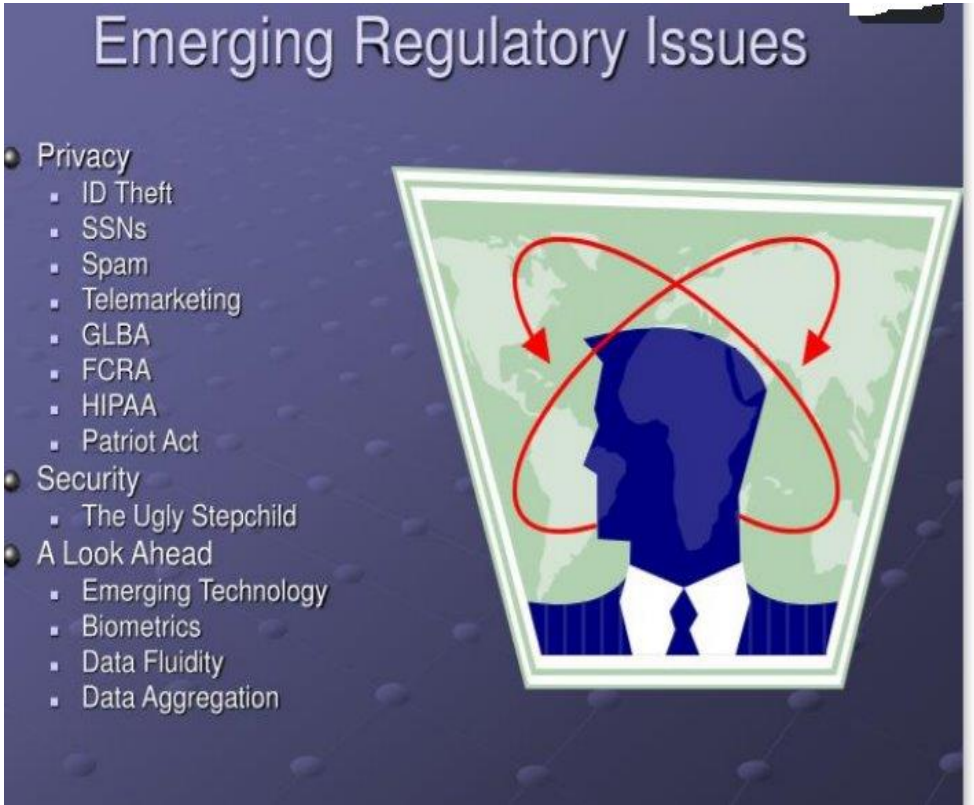


Rial and Danezis (2011)

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Privacy Challenges in Modern Tech

- Cloud, IoT, AI privacy risks.
- Example: IoT smart TV leaks private conversations.
- Exercise: IoT vs Cloud → IoT riskier.
- Conclusion: Recognize new privacy risks.
- Image: https://tse4.mm.bing.net/th/id/OIP.czK9d8gO697s4YP7VvXfVAHaEH
- Reference: Yang et al., AI-driven Anonymization (2024).



Tishk International University
Faculty of Applied Science
Cybersecurity Department

Balancing IoT's Innovations with Privacy and Security Risks

The Internet of Things (IoT) has seamlessly integrated into our lives, promising unmatched convenience, efficiency, and innovation. From transforming homes into smart ecosystems to revolutionizing mobility with connected vehicles, IoT devices have become ubiquitous. Yet, this technological advancement comes with its own set of challenges, particularly concerning privacy and cybersecurity.

Let us use our Smart TVs as the perfect example of this in action. For several smart TV manufacturers, security is an afterthought, which makes them vulnerable to various kinds of threats. Hackers can not only control your unsecured TV for changing channels or volume controls, but also stalk your everyday movements and conversations using the integrated camera and microphone. Why? Because it is far easier to hack into a Smart TV than a far more protected smartphone. And because your TV is connected to your Wi-Fi, hackers can soon gain access to your entire system.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

The Hidden Risks Behind the Technology Powering Smart TVs

Smart TVs epitomize the double-edged sword of IoT technology. Several manufacturers prioritize innovation over security, leaving devices susceptible to various cyber threats. Unsecured smart TVs offer hackers a window, not only to tamper with your viewing experience but also to intrude into your private life through built-in cameras and microphones. The relative ease of hacking a smart TV compared to more secure devices like smartphones, coupled with their connection to your home Wi-Fi, paves the way for hackers to potentially access your entire home network.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Show me the harm...

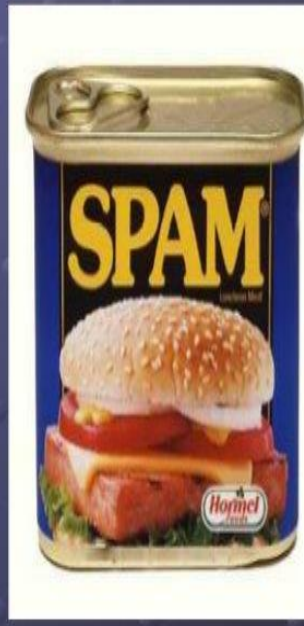
Identity Theft

- FTC Complaints:
  - 2000: 31,000
  - 2001: 86,000
  - 2002: 162,000
  - Top consumer fraud complaint in 2002
  - 30% growth predicted going forward
- Average impact:
  - $1500
  - 175 hours of clean up
  - credit disruptions
- 42% of complaints involve credit card fraud

Identity theft coverage now available

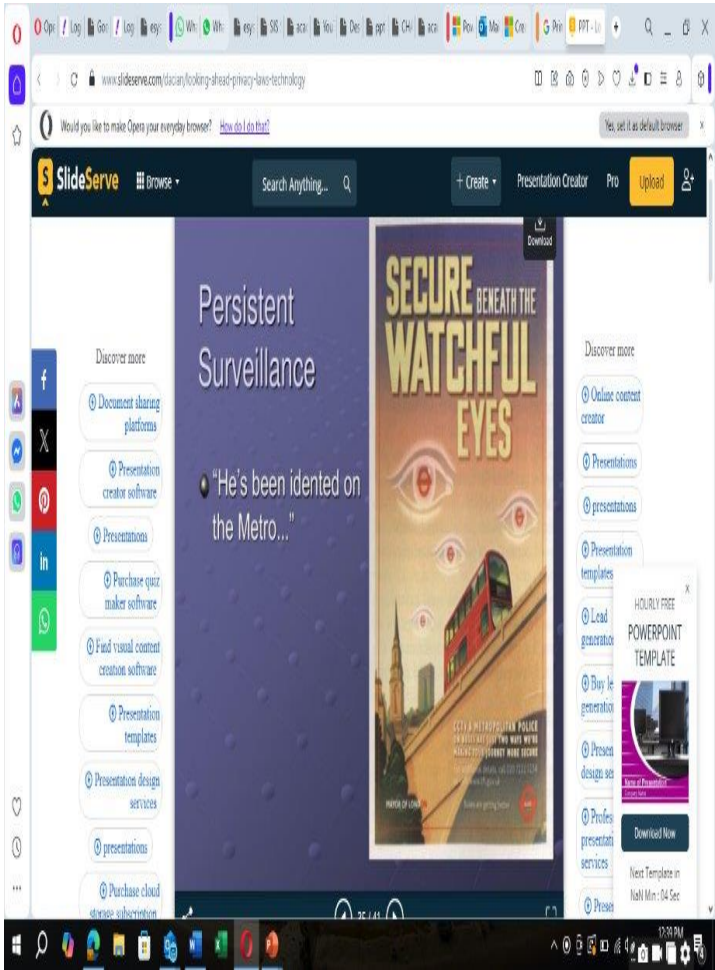
SPAM

- Hotmail – 80% unsolicited bulk email
- 31 billion per day (2002)
- 60 billion per day(2006)
- Dial up concerns (EU local call problems)
- Work productivity/liability concerns
- Deliverability concerns
- Channel viability concerns (the "900" phenomenon)



Tishk International University
Faculty of Applied Science
Cybersecurity Department

Tishk International University
Faculty of Applied Science
Cybersecurity Department

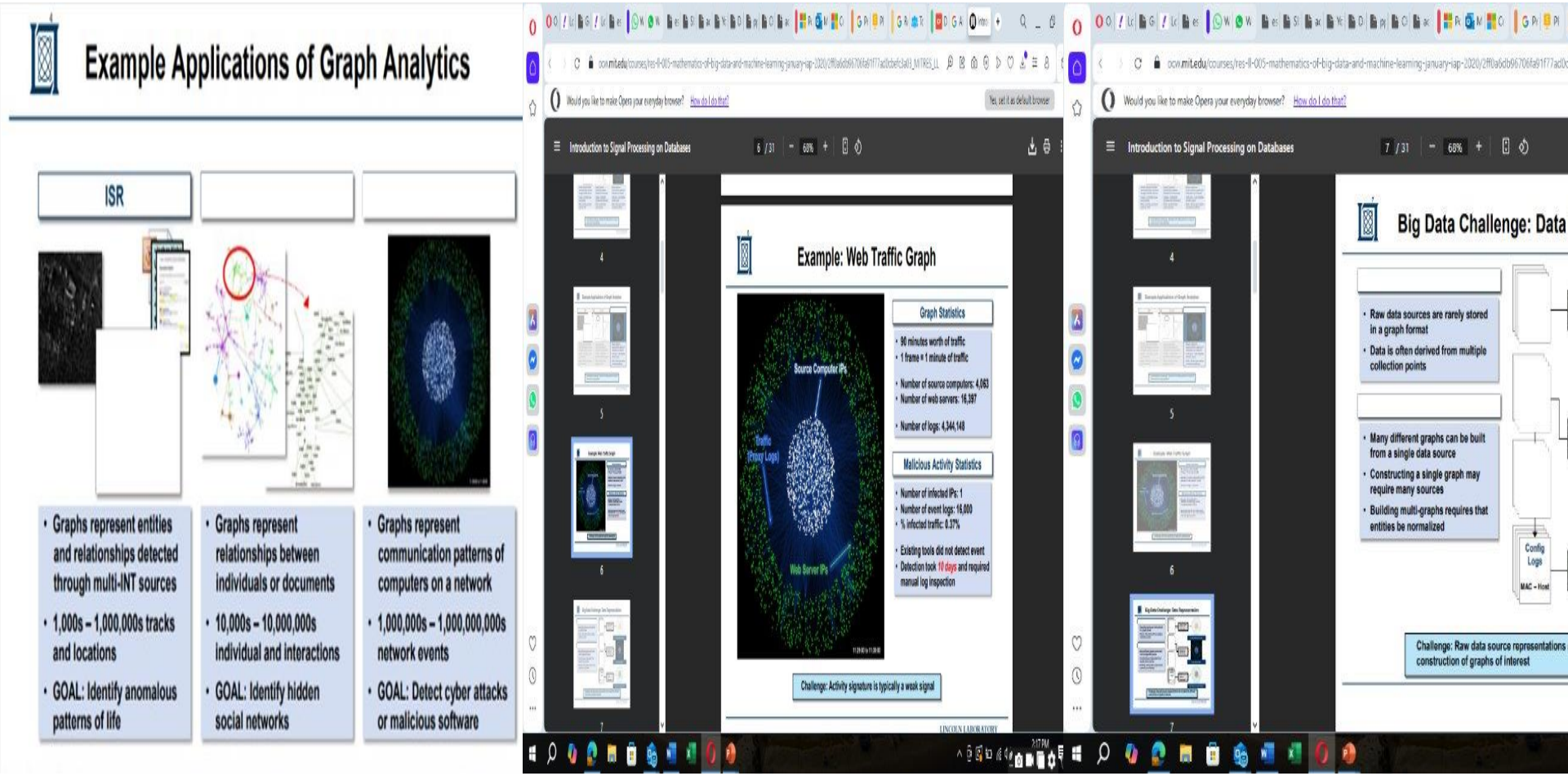


Tishk International University
Faculty of Applied Science
Cybersecurity Department

Case Study: Cambridge Analytica

- Facebook quiz app harvested user & friend data.
- Used for political profiling without consent.
- Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach
- This article is more than 7 years old
- Whistleblower describes how firm linked to former Trump adviser Steve Bannon compiled user data to target American voters
- ‘I made Steve Bannon’s psychological warfare tool’: meet the data war whistleblower
- Mark Zuckerberg breaks silence on Cambridge Analytica

Tishk International University
Faculty of Applied Science
Cybersecurity Department



https://ocw.mit.edu/courses/res-ll-005-mathematics-of-big-data-and-machine-learning-january-iap-2020/2ff0a6db96706fa91f77ad0cbefc3a03_MITRES_LL_005F12_Lec0.pdf

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Balancing Privacy & Security

- Governments argue surveillance increases security.
- Ethical dilemma: Security vs Privacy tradeoff.
- Exercise: Debate if surveillance justified for terrorism.
- Conclusion: Balance must be ethically justified.
- Image: https://cdn-icons-png.flaticon.com/512/3063/3063829.png
- Reference: Richards, Intellectual Privacy (2021).

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Problems & Homework

Homework 1: Essay on opt-in vs opt-out consent.

Homework 2.1: Right to erasure case study.

Homework 2.2: Re-identification risk in health data.

Capstone: Cambridge Analytica ethical/legal analysis.

Solutions provided in notes.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Future of Privacy

AI, IoT, Quantum computing challenges.

Image:
https://tse1.mm.bing.net/th/id/OIP.5Ctk05KyyVEm1X4COF2C8AHaEx

Conclusion: Students anticipate future privacy challenges.

Reference: Fioretto et al., Differential Privacy Overview (2024).

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Importance of Privacy in the Digital Era

In the digital era, personal data has become an incredibly valuable commodity. The vast amounts of data generated and shared online daily have enabled businesses, governments, and organisations to gain new insights and make better decisions. However, this data also contains sensitive information that individuals may not want to share or organisations have used without their consent. That is where privacy comes in.

Privacy is the right to keep personal information confidential and free from unauthorised access. It is an essential human right that ensures individuals have control over their personal data and how it is used. Today, privacy is more important than ever as the amount of personal data collected and analysed continues to grow.

Privacy is crucial for a variety of reasons. For one, it protects individuals from harm, such as identity theft or fraud. It also helps to maintain individual autonomy and control over personal information, which is essential for personal dignity and respect. Furthermore, privacy allows individuals to maintain their personal and professional relationships without fear of surveillance or interference. Last but not least, it protects our free will; if all our data is publicly available, toxic recommendation engines will be able to analyse our data and use it to manipulate individuals into making certain (buying) decisions.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Privacy Challenges in the Age of AI

AI presents a challenge to the privacy of individuals and organisations because of the complexity of the algorithms used in AI systems. As AI becomes more advanced, it can make decisions based on subtle patterns in data that are difficult for humans to discern. This means that individuals may not even be aware that their personal data is being used to make decisions that affect them.

The Issue of Violation of Privacy

While AI technology offers many potential benefits, there are also several significant challenges posed by its use. One of the primary challenges is the potential for AI to be used to violate privacy. AI systems require vast amounts of (personal) data, and if this data falls into the wrong hands it can be used for nefarious purposes, such as identity theft or cyberbullying.

The Issue of Bias and Discrimination

Another challenge posed by AI technology is the potential for bias and discrimination. AI systems are only as unbiased as the data they are trained on; if that data is biased, the resulting system will be too. This can lead to discriminatory decisions that affect individuals based on factors such as race, gender, or socioeconomic status. It is essential to ensure that AI systems are trained on diverse data and regularly audited to prevent bias.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

The Issue of Job Displacements for Workers A third challenge posed by AI technology is the potential for job loss and economic disruption. As AI systems become more advanced, they are increasingly capable of performing tasks that were previously done by humans. This can lead to job displacement, economic disruption in certain industries, and the need for individuals to retrain for new roles.

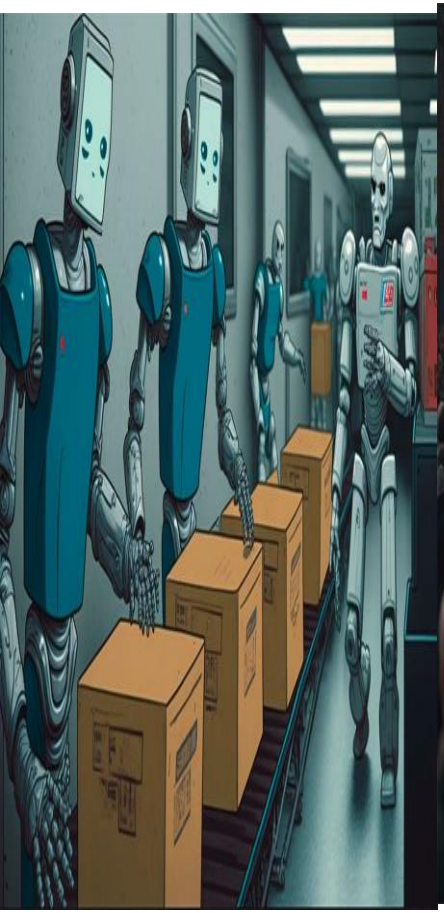
The Issue of Data Abuse Practices

Finally, another significant challenge posed by AI technology is the potential for misuse by bad actors. AI can be used to create convincing fake images and videos, which can be used to spread misinformation or even manipulate public opinion. Additionally, AI can be used to create highly sophisticated phishing attacks, which can trick individuals into revealing sensitive information or clicking on malicious links.

The creation and dissemination of fake videos and images can have serious privacy implications. This is because these fabricated media often feature real people who may not have consented to their image being used in this way. This can lead to situations where individuals are harmed by the dissemination of fake media, either because it is used to spread false or damaging information about them or because it is used in a way that violates their privacy.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

The Issue of Job Displacements for Workers



Underlying Privacy Issues in the Age of AI

The Use of AI in Surveillance

AI-related Privacy Concerns: Real-life Examples

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Solutions to Overcome These Challenges

As we continue to integrate AI into various aspects of our lives, it is clear that privacy and ethical considerations are becoming increasingly important. The potential benefits of AI are vast, but so are the risks associated with its use. As a society, we must take a proactive approach to address these challenges to protect individual privacy and ensure that AI is used ethically and responsibly.

Organisations and companies that use AI must prioritise privacy and ethical considerations in their AI systems' design and implementation. This includes being transparent about data collection and usage, ensuring data security, regularly auditing for bias and discrimination, and designing AI systems that adhere to ethical principles. Companies that prioritise these considerations are more likely to build trust with their customers, avoid reputational damage, and build stronger relationships with their stakeholders.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

As AI continues to advance and transform the world, it is crucial that we do not lose sight of the importance of privacy and ethical considerations.

By prioritizing privacy and adopting strong data protection policies, we can help ensure that AI technology is developed and used in a way that respects individual privacy and other ethical considerations.

Privacy is a fundamental human right, and as AI technology continues to advance, it is critical that we prioritize privacy and ensure that individuals' rights are protected.

This requires a multifaceted approach that involves the cooperation of governments, organizations, and individuals. Governments should implement regulations to ensure that AI is developed and used in a way that respects individual privacy and other ethical considerations. Organizations should prioritize privacy as a core value and adopt strong data protection policies that respect individual privacy.

Finally, individuals should be empowered with transparency and control over their personal data. By prioritising privacy and adopting strong data protection policies, we can help ensure that AI technology is developed and used in a way that is both effective and privacy-respecting, ultimately leading to a future where individuals can benefit from the transformative power of AI without sacrificing their fundamental right to privacy.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Summary & References

- Privacy = ethical + legal duty.
- Laws: GDPR, HIPAA, CCPA.
- Principles: consent, minimization, accountability.
- Future: AI, IoT, quantum risks.
- Main References:
- Solove & Schwartz, Information Privacy Law, 8th Ed. (2024).
- Solove & Schwartz, Consumer Privacy and Data Protection, 4th Ed. (2024).
- Greenleaf, Global Data Privacy Laws (2024).
- Fioretto et al., Differential Privacy (2024).
- Yang et al., AI-driven Anonymization (2024).
- Stallings, Cryptography & Network Security.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Thank you for your listening