WM3E7-15 Privacy and Online Rights

27/28

Department
WMG
Level
Undergraduate Level 3
Module leader
Elzbieta Titis
Credit value
15
Module duration
30 weeks
Assessment
100% coursework
Study location
University of Warwick main campus, Coventry

Description

Introductory description

Privacy is recognised as a fundamental human right, which however can be easily exploited in the digital domain due to the large scale of use and spread of advanced digital technologies for data mining and surveillance. Privacy enhancing technologies (PETs) are designed to minimise personal data use, maximise security and give individuals control of their data. Without that control malevolent actors can manipulate one's identity to serve their goals, with threats to individual privacy involving personal space intrusions, emotional manipulation, and physical interference, including spam emails and retargeting practices. On a large scale, the use of one’s identity and personal information can have severe impact on fundamental rights and democratic processes, meaning secure system should not only protect confidentiality of information, but also support freedom of speech and individuals’ autonomy of decision and self-determination.

As a result, technology companies, governments, and civil society must work together to find adequate solutions to online manipulation and lack of data privacy. In response to regulatory and consumer actions, companies might either comply with privacy rules, employing a reactive response that treats privacy as a compliance issue, or engage in privacy innovation (proactive response), viewing privacy as a core business value which potentially shapes new structures. This creates trade-offs and tensions in privacy and data that characterise regulatory–consumer–company interactions.

The primary goal of this module is to introduce students to the concepts and technologies for

engineering systems that inherently protect users' privacy. Three different privacy paradigms will be introduced, including privacy as confidentiality, privacy as control, and privacy as transparency, alongside technologies that underpin these paradigms, i.e., privacy technologies that keep data confidential, limit the use of disclosed data, and show digital footprint while supporting accountability. Students will be provided with the ability to identify privacy problems, to describe them from a technical perspective, and to select adequate technologies to eliminate, or at least, mitigate these problems. In addition, persuasive system design approach will be also introduced in the context on online privacy, including persuasive principles for enhancing usability of privacy interactions. The secondary goal is to introduce students to wider privacy issues in cyber security, including the common interests and tensions between privacy and cyber security, and considering how cyber security policy can affect privacy, as well as how privacy technologies can be used as double-edge sword by either supporting democracy or anti-social behaviours.

Disclaimer

Solutions to selectively revoke the protection provided by privacy technologies (i.e., adding backdoors or escrow possibilities to ease law enforcement) will not be covered as being strongly discouraged by the privacy researchers and practitioners alike. Moreover, many of the privacy technologies introduced in this module rely on the cryptographic concepts, which however will not be taught in this module. Familiarity with these basic concepts and cryptographic definitions and common primitives is therefore beneficial but not necessary to grasp the material since the focus is on more high-level perspectives as opposed to technical analysis.

Module aims

This module aims to provide the students with a critical awareness of privacy issues in cyber security and allow them to apply advanced technical concepts and practices for managing privacy in organisations using a psychological and usability perspectives.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

The syllabus will include (but is not limited to):

- Definitions and theories of privacy.
- Threats to privacy online and tools for protecting privacy.
- Technologies for ensuring privacy confidentiality, control, and transparency.
- Strategies for designing and implementing privacy-preserving systems.
- Persuasive system design approach for enhancing privacy.
- Privacy laws and standards.
- Moral and cultural perspectives on privacy.

Learning outcomes

By the end of the module, students should be able to:

- Select and critically evaluate the concepts and technologies for engineering systems that inherently protect users' privacy.
- Identify privacy problems and describe them from a technical perspective, and select adequate technologies to eliminate, or at least, mitigate these problems.
- Critically evaluate the relationship between security and privacy, including the role of privacy technologies in enhancing cyber security.
- Critically analyse trade-offs and tensions between reactive and proactive responses to treating privacy issues that characterise regulatory–consumer–company interactions.

Interdisciplinary

The module uses insights from Psychology and Sociology to understand usability issues, human behaviour, requirements gathering and innovation processes relevant for privacy. It also covers existing laws and policies enacted to uphold privacy and data security. Lastly, the module incorporates elements of environmental ethics, accounting for the way in which moral debates shape privacy requirements and how these debates are themselves affected by information technology.

International

The module upholds a global perspective to privacy, covering international privacy laws and standards, as well as cross-cultural privacy differences that have been reported in privacy research, viewing privacy as a cultural phenomenon. As such, the module briefly reviews the concept of culture, discusses the cross-cultural differences in privacy management, and recommends design implications in the international context.

Subject specific skills

- Knowledge of privacy issues as they pertain to cyber security.
- Psychology and usability perspectives to devising and evaluating systems for protecting users' privacy.
- Awareness of relevant areas of research including controversy and progress.

Transferable skills

- Researching literature.
- Communication, critical thinking, and problem solving.
- Time management and teamwork.

Study

Study time

Type	Required
Lectures	18 sessions of 1 hour (12%)
Seminars	18 sessions of 1 hour (12%)
Private study	54 hours (36%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Independent activity between workshops, following up on activities initiated in previous workshops or preparing for upcoming workshops.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A

	Weighting	Study time	Eligible for self-certification
Assessment component			
Impact assessment for privacy risks	50%	25 hours	Yes (extension)

The report will be focused on conducting an initial impact assessment for a real-world system to: a) identify existing challenges for privacy; and b) suggest changes to the system's design to minimize or completely avoid these potential risks. This will include: a) identifying risks to privacy composed by feared events and the actual threats that make these events possible; b) conducting risk assessment using risk mapping (severity and likelihood of risks); and c) proposing mitigations measures to address the privacy risks associated with the system.

Reassessment component			
Impact assessment for privacy risks			No

The report will be focused on conducting an initial impact assessment for a real-world system to:

	Weighting	Study time	Eligible for self-certification

a) identify existing challenges for privacy; and b) suggest changes to the system's design to minimize or completely avoid these potential risks. This will include: a) identifying risks to privacy composed by feared events and the actual threats that make these events possible; b) conducting risk assessment using risk mapping (severity and likelihood of risks); and c) proposing mitigations measures to address the privacy risks associated with the system.

Assessment component

Trade-offs and tensions in privacy responses	50%	35 hours	Yes (extension)

Students will be asked to analyse trade-offs and tensions between various responses to treating privacy issues (regulatory–consumer–company) using case-study approach to draw links between theory and practice, and to learn and evaluate how various people responded to particular complex situations to propose better change in the future.

Reassessment component

Trade-offs and tensions in privacy responses			No

Students will be asked to analyse trade-offs and tensions between various responses to treating privacy issues (regulatory–consumer–company) using case-study approach to draw links between theory and practice, and to learn and evaluate how various people responded to particular complex situations to propose better change in the future.

Feedback on assessment

Written feedback for each assignment.
Verbal feedback during tutorial sessions.
Summative feedback on assignments.

Availability

Courses

This module is Core optional for:

- UWMA-H651 Undergraduate Cyber Security
  - Year 3 of H651 Cyber Security
  - Year 3 of H651 Cyber Security
  - Year 3 of H651 Cyber Security