DEREE COLLEGE SYLLABUS FOR: **PH 3036 LE PRIVACY, POLICY, LAW AND TECHNOLOGY** (Same as ITC 3036) (Updated Fall 2021)	**3/0/3** **UK LEVEL: 5** **UK CREDITS: 15**
PREREQUISITES:	None.
COREQUISITES:	None.
CATALOG DESCRIPTION:	An examination of policy issues and theoretical frameworks to privacy and security. Privacy threat models and privacy protective technologies. Philosophical approaches and legal functions on information privacy. GDPR.
RATIONALE:	The purpose of the course is to provide students with a broad understanding of the breadth, diversity and importance of privacy and policy as it relates to technology and information systems. It is suitable for every student who has an interest in issues of information privacy and cybersecurity.
LEARNING OUTCOMES:	As a result of taking this course, the student should be able to: 1. Demonstrate understanding of the problem of information privacy and the challenges of information evaluation in the contemporary environments of digital security. 2. Demonstrate understanding of the underlying debates and theories about the impact information technology has on privacy and security. 3. Evaluate the social and legal dimensions of information privacy in the context of cybersecurity. 4. Examine the moral implications of information privacy in the context of cybersecurity.
METHOD OF TEACHING AND LEARNING:	In congruence with the teaching and learning strategy of the college, the following tools are used: • Classes consist of lectures and interactive learning (class discussions on contemporary or past events, as well as case studies assigned by the instructor). • Office hours: Students are encouraged to make full use of the office hours of their instructor, where they can discuss the course material. • Use of a Blackboard site, where instructors can post lecture notes assignment instructions, timely announcements, and additional resources. • Use of library facilities: Students are encouraged to make use of the library facilities for their case study assignments as well as for preparation for the final.
ASSESSMENT:	**Summative**:

1st assessment: Midterm Exam (1 hour) Essay-type questions	**30%**
2nd assessment: Portfolio of student work and oral assessment (not eligible for 2nd marking)	**10%**
Final assessment: Research paper 2,300 - 2,500 words)	**60%**

Formative:

In-class or take-home diagnostic assignments	**0%**

The formative assessments aim to shape teaching and prepare students for the summative assessments.
The 1st summative assessment tests the LOs 1 and 2.
The 2nd summative assessment tests the LOs 1-4.
The final summative assessment tests the LOs 1-4.

The final assessment tests all learning outcomes of this module, therefore students pass the module if the average module grade is 40% or higher.

INDICATIVE READING:

REQUIRED READING:

1. Kesan, Jay P. and Hayes, Carol. (2019). *Cybersecurity and Privacy Law in a Nutshell*. West Academic Publishing.
2. Solove, D.J., Rotenberg, M. and Schwartz, P.M., (2006). *Privacy, Information, and Technology*. New York: Aspen Publishers.

RECOMMENDED READING:

1. Arcos, R & Pherson, R., eds. (2015). *Intelligence Communication in the Digital Era*. Basingstoke: Palgrave Macmillan.
2. Castells, M. (2010). *The Rise of the Network Society*. Blackwell Publishers.
3. Clarke, R. & Knake, R., (2012). *Cyber War: The Next Threat to National Security and What to do About it*. New York: Harpercollins.
4. DeCew, J. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca: Cornell University Press.
5. Fried, C. (1970). *An anatomy of values*. Cambridge, MA: Harvard University Press.
6. Gusterson, H., (2017). *Drone: Remote Control Warfare*. MIT Press.
7. Inness, J. (1992). *Privacy, Intimacy and Isolation*. Oxford, UK: Oxford University Press.
8. Lampert, Paul. (2018). *Understanding the New European Data Protection Rules*. CRC Press.
9. Moore, A. D. (2010). *Privacy Rights: Moral and Legal Foundations*. University Park, PA: Penn State University Press.
10. Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.
11. Rappert, Brian (2007). *Technology and Security: Governing Threats in the New Millennium*. Palgrave Macmillan.
12. Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy*. Chapel Hill, NC: The University of North Carolina Press.
13. Richards, J. (2014). *Cyber War: The Anatomy of the Global Security Threat*. Palgrave Macmillan.
14. Richardt, A et al., eds. (2013). *CBRN Protection: Managing the Threat of Chemical, Biological, Radiological and Nuclear Weapons*. Weinheim: Willey.
15. Roessler, B. (2005), *The Value of Privacy*, Cambridge, MA: Polity Press.
16. Schoeman, F. (1984). *Philosophical dimensions of privacy: An anthology*. Cambridge: Cambridge University Press.
17. Tavani, T. H. (2007). *Ethics and technology: Ethical issues in an age of information and communication technology*. New York, NY: John Wiley & Sons.

	18. Trottier, D and Fuchs, C., (2014). *Social Media, Politics and the State*. New York: Routledge. 19. Voigt, Paul & Axel von dem Bussche (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International. 20. Westin, A. (1967). *Privacy and freedom*. New York, NY: Atheneum.
INDICATIVE MATERIAL: *(e.g. audiovisual, digital material, etc.)*	**REQUIRED MATERIAL**: N/A **RECOMMENDED MATERIAL**: N/A
COMMUNICATION REQUIREMENTS:	Verbal skills using academic / professional English.
SOFTWARE REQUIREMENTS:	Microsoft Word
WWW RESOURCES:	http://noesis.evansville.edu/ http://plato.stanford.edu/ http://www.iep.utm.edu
INDICATIVE CONTENT:	- Introduction - Perspectives on Privacy a. The Philosophical Discourse about Privacy (Solove et al) b. Ancient philosophical approaches to Privacy (Aristotle, Plotinus, Augustine) c. The Definition and Value of Privacy (Roessler) d. The Right to Privacy (Locke, Kant) e. The feminist perspective on Privacy f. Information privacy and self-determination (Westin) g. Foucault on Privacy (Discipline and Punishment) h. Critics of Privacy i. Critical survey of predominant approaches to Privacy (Nissenbaum) - The Ethics of Privacy (contemporary moral debate) - Privacy, Algorithms, and Artificial Intelligence - Privacy and the Media a. Information Gathering b. Disclosure of Truthful Information c. Dissemination of False Information d. Appropriation of Name or Likeness e. Privacy protection for Anonymity and Receipt of Ideas - National Security and Foreign Intelligence a. The Intelligence Community b. The Fourth Amendment Framework c. Foreign Intelligence Gathering d. NSA Surveillance e. EU Legislation and International Privacy Law (GDPR) - Health Privacy a. Confidentiality of Medical Information b. Constitutional Protection of Medical Information c. Genetic Information d. Informed Consent - Government Records (Politics and Privacy) a. Public Access to Government Records (e-Government)

	b. Government Records and Use of Personal Data c. Sensitive Data and Identity Theft - Education Privacy a. School Searches and Surveillance b. School Records - Employment Privacy