PhD RESEARCH – IN PROCESS

Request to be included

If you are currently doing a PhD regarding an element of electronic evidence and electronic signatures, and would like to have your details added to our Current Research section, please download and complete a submission form (docx) and send by email to: stephenmason@stephenmason.co.uk

Candidates taking PhDs

Name of candidate: **Jessica Shurson**

University at which the PhD is registered and the awarding institution: Queen Mary University of London

Department or faculty: Centre for Commercial Law Studies

Title of the degree: PhD

Title of the thesis:

> Legal Jurisdiction and the Globalization of Evidence: A Theory of Data Sovereignty for Law Enforcement Access to Data Across Borders

Brief description:

With the rise in cloud computing, law enforcement is increasingly in need of digital evidence stored across borders. This data is often controlled by US service providers, or physically located in a data center, outside of the jurisdiction. The current system for cross-border data requests, mutual legal assistance treaties (MLAT), is incapable of meeting the increasing demand for digital evidence, resulting in unworkable delays in accessing evidence for the investigation of serious crime. As a result, governments may turn to hacking, unilateral extraterritorial reach of production orders, and data localization, to access digital evidence more easily. These methods can lead to foreign policy tensions, a splintering and inefficient internet, and possible human rights' abuses. New reforms have emerged in the US and Europe to address deficiencies in the MLAT system but have yet to be implemented.

This thesis will begin by considering the concerns of stakeholders involved – law enforcement, service providers, and data subjects – and the nature of data and technology of cloud computing. By engaging in a comparative analysis of areas of transnational law that involve similar conflicts of law and conducting a doctrinal analysis of well-accepted doctrines of sovereignty and jurisdiction under public international law, this thesis will formulate a theory of data sovereignty for law enforcement access to data across borders. This thesis will then utilize this theory of data sovereignty to critically assess emerging approaches to reform the MLAT system, including the US Cloud Act, the Council of Europe Cybercrime Convention Additional Protocol, and the EU E-Evidence Proposal. Ultimately, the thesis will determine whether these principles of data sovereignty can be utilized to identify a harmonized approach to law enforcement access to cross-border data that simultaneously: (1) offers enhanced certainty to internet service providers by eliminating conflicts of laws; (2) respects individual privacy and other human rights; and (3) recognizes sometimes overlapping, yet legitimate, state interests in accessing and protecting data.

Supervisors: Professor Ian Walden and Professor Julia Hörnle

Date of registration: October 2018

Name of candidate: **Jessica Schroers**

Contact e-mail: Jessica.schroers@kuleuven.be

https://www.law.kuleuven.be/citip/en/staff-members/staff/00089696

University at which the PhD is registered and the awarding institution: KU Leuven – University of Leuven

Department or faculty: Faculty of Law, Centre for IT & IP Law (CiTiP)

Title of the degree: PhD

Title of the thesis:

Responsibility for online identity

Brief description:

Off-line we have generally accepted ways of identifying persons, for instance by looking them in the face and checking the pictures on their identity cards. Online, these traditional identification procedures cannot be performed in a feasible manner. Therefore other technological possibilities are used, often provided by a third party, an identity provider. In part due to the particular features of the online identification procedures, and in part due to lack of consideration by legal scholars, it is not clear to what degree and under which circumstances a person is responsible for what is done with her online identity. The eIDAS Regulation, for instance, which provides general rules for electronic identification and trust services, does not cover liability rules regarding private identity providers; it specifies only very limited provisions regarding governmental identity providers. Subsequently, the liabilities of the identified person are unclear as well. This research analyses the liability allocation of the participants involved in the online identification process, with a focus on the position of the identified natural person whose online identity is used in case of incorrect online identification. The research aims to give a well underpinned legal account of how a liability position of this natural person can be achieved that at least comes close to the existing liability position of persons in case of misuse of their banking information in the banking sector.

Supervisors: Professor Anton Vedder and Professor Peggy Valcke (co-supervisor)

Date of registration: 11 April 2018

Name of candidate: **Alfonso Delgado De Molina Rius**

Contact: a.delgado17@imperial.ac.uk

University at which the PhD is registered and the awarding institution: Imperial College London

Department or faculty: Computer Science

Title of the degree: PhD

Title of the thesis**:**

Split Contracts: Bridging Legal Prose and Smart Contract Code

Brief description:

My research involves creating split contracts that are governed by both natural language and smart contract code. The aim is to combine the strengths of each medium to create legally binding agreements that can be executed algorithmically. I also research the practical applications of smart contracts in diverse industries to identify value-creation opportunities.

Supervisor: Professor Michael Huth

Date of registration of the PhD: October 2017

Name of candidate: **Tõnu Mets**

University at which the PhD is registered and the awarding institution: Tartu Ülikool (University of Tartu)

Department or faculty: Õigusteaduskond (School of Law)

Title of the degree: PhD

Title of thesis:

Applicability of general rules of evidence to digital evidence

Brief description:

The thesis focuses on the different criteria for admissibility of digital evidence in a legal setting. It is based on the analysis of existing evidence law and the practice of applying general rules of evidence to digital evidence. Proposed and emerging legislation for digital evidence will be analysed and a national solution developed for the procedural laws in Estonia.

Supervisors: Professor Irene Kull and Professor Raimundas Matulevičius

Date of registration: 2016

Date of submission: 2020

Name of candidate: **Kristel De Schepper**

University: Catholic University of Leuven, Belgium

Department or faculty: Faculteit Rechtsgeleerdheid, Instituut voor Strafrecht (Law Faculty, Institute of Criminal law)

Title of degree: PhD

Title of the thesis:

Strafbaarstelling van spionage en informatiemisbruik ter bescherming van bedrijfsgeheimen

Criminalisation of espionage and information abuse to protect business secrets

Brief description:

Het strafrecht koppelt negatieve gevolgen aan de schendingen van rechtsgoederen en mag daarom pas als laatste redmiddel worden ingezet. In een informatiemaatschappij nemen deze rechtsgoederen steeds meer een immateriële vorm aan (dematerialisering). Deze dematerialisering daagt het strafrecht uit. Bij het strafbaar stellen van gedragingen (en bijgevolg het beschermen van rechtsgoederen) lijkt de normgever de neiging te hebben om te focussen op de al dan niet materiële vorm of op de fysieke drager van goederen. De vraag rijst of hij hierdoor de inhoud van de informatie niet teveel op de achtergrond plaatst. De vorm zal immers steeds minder belangrijk worden naargelang de samenleving (en haar rechtsgoederen) steeds meer wordt geïnformatiseerd. Daarnaast kan de inhoud ook belangrijk zijn terwijl deze net moeilijker te beschermen is door de informatisering.

Dit onderzoek gaat uit van het vermoeden dat de normgever bij de strafbaarstelling meer aandacht moet hebben voor het type rechtsgoed dat hij wil beschermen. Aan de hand van een gevalstudie van de strafrechtelijke bescherming van bedrijfsgeheimen, onderzoeken we of een betere focus op het begrip rechtsgoed bij de strafbaarstelling niet tot betere wetgeving kan leiden en zo bijdragen tot de toepassing van het strafrecht als laatste toevlucht.

Criminal law incriminates behaviour which violates legal interests, but only as a last resort. Is our criminal law up to the challenges of the information society? In an information economy a different approach towards the protection of valuable corporate information should be considered. Management and corporate policy decisions nowadays are taken in the 'virtual world', and economically valuable information is increasingly stored on digital data systems. Secret corporate information can be very valuable and as such worth protecting against espionage by insiders or outside competitors.

Existing offences relate to the illegal access, use or abuse of corporate (digital) information and hence they often focus on the means used to access the data, rather than on their actual content.

The research hypothesis is that a focus on and a sharper definition of the legal good protected by specific offences, will lead to more respect for the idea of criminal law as the ultimate resort and to a more efficient use of criminal law.

On the basis of a case study of corporate espionage and the violation of corporate secrets, the research intends to establish the criteria which should guide lawmakers considering the creation and use of criminal law. It hopes to illustrate how these criteria interact in the pursuit of the criminal protection of information as an ephemeral, itinerant and sometimes opaque legal interest.

Supervisor: Professor dr. Frank Verbruggen

Date of registration: 1 September 2011

Anticipated date of submission: 1 September 2016