PhD Candidate: Legal Cybersecurity and Privacy Obligations for the Internet of Things

As our world is becoming increasingly digitalized, the Internet of Things (IoT) is growing rapidly. While the IoT has important and useful functions, it also presents serious cybersecurity and privacy risks. As a PhD candidate, you will critically evaluate the current legal framework in relation to cybersecurity and privacy obligations for IoT and provide recommendations for future rules. This way, we can work towards safer digital ways to enhance our life and work.

We are looking for a PhD candidate in law. The project concerns legal cybersecurity and privacy obligations in relation to IoT devices. The Internet of Things (IoT) consists of many devices that are connected to each other and the internet. The IoT surrounds us with a network of smart, interconnected devices and services capable of sensing or even listening to requests or needs, and acting on them.

While the IoT has important and useful functions, it also presents serious cybersecurity and privacy risks. These risks are amplified due to various characteristics of IoT devices. For example, the software of these devices is often only supported for a limited time. This can lead to insecure devices that are not updated but still used. Furthermore, cybersecurity and privacy can depend on many different actors such as the developers of the hardware and software of the IoT device and other connected devices, the controllers of personal data, and the users themselves. In addition, several types of market failures are at play. For instance, the manufacturers and users of IoT devices are often best able to secure the devices, while they lack incentives to do so.

The European Union has adopted and proposed many legal rules in relation to cybersecurity and privacy. Nevertheless, problems remain, especially in the IoT context. For example, the EU rules do not provide clear rules on the distribution of responsibility when cybersecurity and privacy depend on multiple parties. Furthermore, the current legal framework is fragmented and inconsistent. It contains many obligations, but they are limited to specific situations, risks and actors. For these reasons, legal cybersecurity and privacy obligations may not always be effective.

The aim of this project is to analyse and critically evaluate the current legal framework in relation to cybersecurity and privacy obligations for the internet of things, and to provide recommendations for future rules. The exact research question will be formulated in collaboration with the supervisors. It is also possible to formulate a more specific question related to this broader topic. Your teaching load may be up to 10% of your appointment.

You will be supervised by Prof. Bart Jacobs, Dr Pieter Wolters, and Prof. Frederik Zuiderveen Borgesius.
Profile

- You hold a Master's degree in law.
- You have a demonstrable interest in law and information technology.
- You have an excellent command of written and spoken English.
- You have a good understanding of cybersecurity and privacy, preferably demonstrated by work experience, publications, or a Master's thesis.

We are

As a PhD candidate, you will be affiliated with the iHub, Radboud's interdisciplinary research hub on digitalisation and society. iHub brings together a diverse range of academics from across the humanities, social sciences, engineering, law, and natural sciences to tackle urgent questions raised by the increased digitalisation and datafication of science and society. Digital technologies shape more and more aspects of our lives, from how we work and communicate, to how we live together in cities, participate in politics, promote health and fight disease. As digitalisation expands to all sectors of society, governance of science and technology becomes increasingly complex, and balancing benefits and risks while negotiating competing interests becomes paramount. iHub's mission is to better understand the effects of digitalisation on our society and to help steer digital transformations in ways where public values are central.