1. Introduction

1.1 INTRODUCTION

These days, it is virtually impossible to pick up a newspaper or watch a news program on TV without coming across some mention of privacy and/or data protection. This is unsurprising given the central role that data play in the world – defined both spatially and temporally – in which we live. Much of the discussions are focussed on, or at least contain elements of, cross-border considerations. In other words, data privacy with a twist of international law has become a very hot topic indeed.

At the time of concluding the writing of this book, the news was filled with discussions of whether Putin’s Russia was behind the hacking activities, and the spread of misinformation, that saw a ‘reality TV’ personality take on the job as President of the United States. On 6 January 2017, the US Office of the Director of National Intelligence released a declassified report combining conclusions from investigations of the FBI, the CIA and the NSA. That report concluded that:

Moscow’s influence campaign followed a Russian messaging strategy that blends covert intelligence operations – such as cyber activity – with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or ‘trolls.’ … Russia’s intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with both major US political parties. … We assess with high confidence that Russian military intelligence (General Staff Main Intelligence Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release US victim data obtained in cyber operations publicly and in exclusives to media outlets and relayed material to WikiLeaks.¹

Looking forward, the report also made the following prediction: ‘We assess Moscow will apply lessons learned from its campaign aimed at the

US presidential election to future influence efforts in the US and worldwide, including against US allies and their election processes.\footnote{2}

All this is a potent reminder of just what is at stake in the international data privacy and security arena. The cyber-environment, in which data are the building blocks, is no longer merely a playground for ‘nerds’. Rather, it is now clearly integrated into the ‘real world’, and distinguishing between the two is no longer meaningful; the real-world implications of activities in the cyberworld are undisputable.

In this book, we elaborate on the concepts of individual data privacy and information sovereignty, which we believe are not only similar but essentially equivalent. In this work, which originally started as an idea for an article or two, we demonstrate that it is possible not just to name their common principles but even to identify a common method to tackle the problems that arise from their inevitable collisions. In addition, we illustrate that it is possible to mutually transfer or transplant existing experiences between these two areas of law to resolve some of their contemporary ‘hard cases’ or fundamental controversies.

The topics of this book are all centred on contemporary ‘hot’ issues of international data privacy and information security. However, while we deal with obvious questions of cross-border data flows etc., our aim goes beyond a mere description of current law and legal practices. We try to show that further exploration of the true nature of individual and international ‘information sovereignty’ might provide not only for solutions of existing problems (e.g. of territoriality) but also for ways to answer new questions yet to arise in the future.

1.2 A DEVELOPING AREA OF GREAT IMPORTANCE

This book elaborates on the assumption that information privacy is, in its essence, comparable to information sovereignty. This – seemingly rudimentary – observation serves as the basis for an analysis of various information instruments in domestic and international law. It also provides for the method to resolve situations where the informational domains of individuals and/or states collide.

There are numerous legal cases where information sovereignty of a state collides with information sovereignty (data privacy) of an individual – for example digital discovery in criminal investigation, data retention...
etc. In these cases, courts use the method of proportionality to assess adequate balance between data privacy and values such as national security or public order. In this book, we argue that such conflicts are, by their nature, arising from the same fundamental concept and should be treated as such.

Even more importantly, understanding the parallels between the regulatory concepts of information sovereignty and data privacy might significantly help in resolving ‘hard cases’ of both of these concepts that do not even include their mutual conflict. Simple analogical transfer of experience with the use of the concept of sovereignty in public international law can, in cases where proper methodology is applied, show the correct ways of resolving difficult legislative or interpretative assignments in privacy, and vice versa.

To demonstrate the analogy between information sovereignty and data privacy, we choose some of the most significant emerging issues of contemporary cyberlaw, including cross-border discovery, cybersecurity and cyber-defence operations, and legal regimes for cross-border data transfers. We do not aim to describe or analyse these relatively distinct issues in depth, but rather we focus on their fundamental problems (which are by their nature, as we believe, very similar) and show ways to resolve them. For instance, in cybersecurity, we use the aforementioned analogy and method to define an alternative concept of the informational component of state sovereignty under public international law – a concept that is not burdened by the logical and technical contradictions of recently dominant territorial understanding of sovereignty and jurisdiction.

The main use for the book is by academic readers ranging from doctoral students to advanced researchers. We hope that the scope of possible audience is relatively broad given that the book tackles, on an abstract level, two concepts that are central to contemporary law of information and communication technologies (cyberlaw), i.e. privacy and sovereignty. In that sense, the ambition of the book is to contribute to further forming of doctrine of both these concepts. As privacy became an integral part of a number of specific legal phenomena, we believe the book might also be of use for those who elaborate on issues like eCommerce, eGovernment, online protection of intellectual property etc. At least equally important for almost all areas of cyberlaw is also the question of sovereignty and its consequent implications such as jurisdiction, law applicable and authoritative enforcement, simply because it is essential for any lawyer to know, prior to approaching some particular legal issue of the online world, which law applies and to which extent.
A unique feature of the book is that both concepts, i.e. information privacy and information sovereignty, are analysed, discussed and developed here using the same core method. The discovery of the possibility of approaching information privacy and information sovereignty through the same methodological paradigms was actually the main impulse that made the authors commence work on the book. Both concepts share the same factual and philosophical basis, but they belong to entirely different areas of law. That is probably also the main reason these concepts have not been used before in close connection. The distance between respective legal disciplines (i.e. privacy law and public international law) also causes particular terminological and doctrinal mismatches that represented the biggest challenge in the process of putting the book together. However, it is possible to overcome these particularities on an abstract level as well as on the level of specific legal issues – which might also per se serve as just another proof of the essential similarity of data privacy and information sovereignty as such.

An equally important impulse for creating the book was our observation of the fundamental contradictions between the content of actual legal rules and the findings of cybernetics and information sciences. While law tends to understand information as a static object, natural information sciences proved that it should be understood as a process (in particular, as a process of organizing various entities). Consequently, we aim at establishing a proper legal understanding of meanings and functions – namely of the core natural concepts of information and data. Apart from theoretical significance, we note that lack of acknowledgement of the natural functional features of information negatively affects the practical efficiency of various legal instruments. In that sense, we choose some negative examples of protection of personal data or cybersecurity, as well as some positive examples of privacy stricto sensu (i.e. the civil law concept of privacy) or intellectual property, to demonstrate that reflecting the true nature of information is essential for practical legitimacy of even very particular and specific legal rules.

1.3 USER GUIDE (HOW TO READ THIS BOOK)

This is a book about ideas. Some of those ideas are fully developed. Others, however, are presented here rather as a starting point for future discussions. For this, and other reasons, we want to conclude this introduction with a disclaimer to the reader:
Caveat Emptor (Legal Disclaimer)

(1) This is a book and should only be used for the purposes for which books commonly are used. Even if it floats, this book is not intended to be used as a flotation device or otherwise for life-saving activities.

(2) The content of this book is based on the following assumptions:
   (a) that information is the opposite of entropy;
   (b) that current technology makes the physical location of data practically irrelevant for many purposes;
   (c) that states as well as individuals have natural rights to claim their informational domains; and
   (d) that the aforesaid rights of states and individuals are essentially equivalent.

If you are allergic to any of these ideas, or otherwise find these assumptions inappropriate or offensive, please do not read further (it just gets worse).

(3) This book is not intended to solve all regulatory problems of contemporary international information society. Some parts of this book might contain traces of pragmatic solutions of most evident regulatory paradoxes of contemporary Internet law. However, the authors accept no liability for any subsequent attempts to apply these solutions in actual legal practice.

(4) This book is not smart (in any sense). It does not contain any sensors, so you might openly and loudly discuss private matters in front of it. By reading this book, you make no waiver of your privacy or intellectual property rights.

(5) This book is a fresh brew. Some ideas might not be fermented properly. Some parts of this book are blended with highly valuable VSOP and Gran Reserva content that does not originate in the minds of the authors. The authors respectfully apologize to those whose great ideas were accidently blended into this book without proper acknowledgment in footnotes or elsewhere.

(6) If you experience difficulties agreeing with any of the ideas presented in this book, please do not be alarmed – it is not your fault. It is a design feature arising from the fact that even the authors were sometimes unable to mutually agree on some things.

(7) If this book still contains attempted anecdotes that might not seem funny to most audiences, it means the publisher was just too kind to edit them out.