Contemporary Voices

On the life and lives of digital data: The US - EU safe harbor framework and beyond

by Katarina Rebello

Abstract

Digital data is entangled in a variety of intersecting discourses and debates- from narratives about 'big data revolutions' and 'open data movements' to controversies surrounding security and surveillance practices as well as divisive questions about privacy and data protection as social and legal principles. This article will unpack digital data from a security perspective within the context of the Safe Harbor Framework, a governance arrangement designed to facilitate digital data flows between the United States and the European Union. The driving focus of this article is best defined through several interrelated questions, namely: What is digital data? How is it possible for digital data to be constructed in overlapping and contested ways? And what does the development and deterioration of the Safe Harbor Framework reveal about the nature of digital data in the contemporary world? This article proposes that digital data is 'alive' and has many 'lives'- simultaneously constructed as a 'mundane' feature of everyday life, as a component of 'security-enhancing' strategies, and as a 'security threat'.

Keywords: Big Data, Data Protection, Open Data, Privacy, Security, Surveillance, Transatlantic

Introduction

Digital data represents the sum of information generated through actions and interactions on the Internet- encompassing everything from emailing and instant messaging to video streaming, online banking, and social networking (Gralla, 2007, p.13). The information generated through these increasingly diverse online activities is converted and stored as digital data using a numerical system of binary code, commonly represented by assorted sequences of 0's and 1's (Lupton, 2015, p.8). The upsurge of global Internet connectivity and the rapid development of Internet-accessible technologies and devices have enabled individuals and communities around the world to be constantly connected to the Internet (Lupton, 2015, p.9). Collectively, these phenomena have resulted in the 'datafication' of contemporary life in the twenty-first century- as digital data is continuously collected, stored, and analyzed around world to produce insights about a wide range of social behaviors (Cukier and the Mayer- Schonberger, 2013, p.78).

In tandem with these ongoing transformations, digital data has become entangled in a variety of intersecting discourses and debates- ranging from narratives about 'big data revolutions' and 'open data movements' to controversies surrounding security and surveillance practices as well as divisive questions about privacy and data protection as social and legal principles. These tensions are nowhere more prominent than within the context of the United States (US) and the European Union (EU). Since the late-twentieth century, the collection, storage, and analysis of digital data have generated notable transatlantic tensions, resulting in a complex legal and regulatory arena (Andrews *et al.*, 2005, p.128). For over 15 years, the US - EU Safe Harbor Framework was unchallenged as the 'gold standard' of data transfer agreements- facilitating digital data flows between the United States and the European Union (Connolly, 2008, p.5). This governance arrangement suddenly deteriorated in October 2015, when the Court of Justice of the European Union (CJEU) invalidated the Safe Harbor Framework, citing concerns that the United States was no longer upholding adequate standards for such an arrangement (Court of Justice of the European Union, 2015). The consequences of this landmark decision placed the future of transatlantic data flows in jeopardy- exposing crucial tensions surrounding digital data in the twenty-first century.

The focus of this article is best defined through several interrelated questions, namely: What is digital data? How is it possible for digital data to be constructed in overlapping and contested ways? And what does the development and deterioration of the US - EU Safe Harbor Framework reveal about the nature of digital data in the contemporary world? In order to explore these questions, this article will unpack digital data from a security perspective. Looking at digital data through a security lens offers a unique entry point into thinking critically about the multiple roles of digital data in modern life. This research does not seek to differentiate between 'good' and 'bad' practices surrounding digital data (Kitchin, 2014b, p.165). Rather, this article will explore the many ways in which digital data are actively shaping and being shaped by our world. Going further, this article proposes that digital data is 'alive' and has many 'lives' simultaneously existing as a 'mundane' feature of everyday life, as a component of 'security- enhancing' strategies, and as a 'security threat'.

Defining Digital Data

It is important to develop conceptual clarity about digital data and consider the primary contexts against which it is understood. In general, the ways that digital data are spoken about have become increasingly complex in recent years, involving many terminologies- each with meaningful social, political, and legal consequences (Aradau, 2010, p.494). Actors that generate digital data are broadly known as 'data subjects' while actors that engage in the collection, analysis, and storage of digital data are known as 'data controllers' (Bygrave, 2014, p.18). The rights and obligations conferred onto data subjects and data controllers largely depend on the definition of digital data. The focus of most contemporary discussions concerns 'personal data', signaling that information may be connected to an identifiable individual possessing specific rights (Kuner, 2013b, p.17). In recent years, however, there have been considerable efforts to distinguish 'personal data' from 'non-personal data' (Rubinstein, 2013, p.74). Non-personal data, often referred to as 'metadata', implies that data has been disaggregated or anonymized so that it can no longer be connected to any one individual, thereby unfastening the rights and obligations associated with personal data (Aradau, 2010, p.493). There are reasons to question these arbitrary distinctions. Among others, Kuner concedes that digital data categorized as 'non- personal' or 'anonymized' can almost always be linked to an individual (Kuner, 2013b, p.18).

In addition to questions about the distinction between 'personal' and 'non-personal' data, there have also been notable efforts to differentiate between 'national' and 'international' data flows- further impacting the respective rights and obligations of data subjects and data controllers. This distinction suggests that digital data may be collected, stored, and analyzed entirely within territorial state borders or that it can flow freely across borders. Such terminologies, however, are largely misleading- failing to recognize how digital data moves and circulates in fluid ways (Dalton *et al.*, 2016, p.6). Some argue that Bigo's analogy of the Mobius strip adequately conveys the blurring of boundaries between the 'inside' and the 'outside' of contemporary data flows (Bauman *et al.*, 2014, p.125). From a more technical perspective, De Hert and others remind us that the Internet is not designed to transmit data on the basis of geographical borders (De Hert *et al.*, 2016, p.26). On this basis, "it may no longer be feasible to differentiate between transborder data flows and those that do not cross national borders" (Kuner, 2013b, p.6).

For the purposes of this article, references to digital data encompass both personal data and non-personal data, recognizing the increasingly blurred distinctions between these terms. This article also contends that digital data flows epitomize a comprehensively transborder phenomenon, thereby resisting efforts to distinguish between national and international data flows. This conceptual orientation is by no means unproblematic. However, such an approach seeks to address the implications of these vocabularies while equally moving beyond them. Building on these foundations, it becomes possible to engage more closely with the overlapping and contested roles of digital data in the contemporary world. The sections below will explore prevailing discourses and debates surrounding digital data within the context of the US and the EU, namely: big data and open data, security and surveillance as well as privacy and data protection in order to lay down the conceptual foundations of this article.

Big Data and Open Data

Recent mentions of 'big data' in discourse and practice seek to differentiate historical uses of digital data from more contemporary developments related to the generation, collection, storage, and analysis of data in the twenty-first century (Cukier and Mayer-Schonberger, 2013, p.6). Definitions of big data commonly include references to the '3 V's': volume, variety, and velocity (Andrejevic, 2014, p.1676). This definition evokes the unprecedented diversity, access, and speed of contemporary data practices while simplifying their technical complexity. The advent of big data technologies is also widely referred to in terms of a 'revolution' (Cukier and Mayer-Schonberger, 2013, p.6). As society generates increasing amounts of digital data, the commercial opportunities to analyze and monetize this information have amplified (Aiden and Michel, 2013, p.11). The rise of data mining, data analytics, and the expansion of data storage facilities worldwide have allowed private sector businesses to accumulate unprecedented quantities of digital data (Walker, 2015, p.7). Big data 'pioneers' like Google, Amazon, and Facebook have benefitted from the ability to convert this digital data information into new forms of economic value (Cukier and Mayer-Schonberger, 2013, p.116). "Data has been figured as a 'gold mine' and as the new oil of the Internet and the new currency of the digital world" (Gitelman, 2013, p.123). Unlike other commodities, however, "data's value does not diminish when it is used; it can be processed again and again" (Cukier and Mayer-Schonberger, 2013, p.101). From this position, "the more data gathered and analyzed, the better" (Lupton, 2015, p.94).

In tandem with these developments, there has been a notable upsurge of data intermediaries and data brokers- creating an entire economy around the collection, sale, and resale of digital data (Kitchin, 2014b, p.42). Examples of these actors include search engines, financial and transactional intermediaries as well as advertising intermediaries (DeNardis, 2014, p.155). Many public and private sector industries employ third-party data intermediaries and data brokers to expedite the process of monetizing digital data generated online (DeNardis, 2014, p.155). Drawing on the prospects of data use and reuse, these activities generally involve consolidating, repackaging, and reselling digital data (Custers and Ursic, 2016, p.8). This has created a "multibillion dollar industry, with vast quantities of data…being rented, bought, and sold daily across a variety of markets- retail, financial, health, tourism, logistics, business intelligence, real estate, private security, political polling, and so on" (Kitchin, 2014b, p.42).

Another offshoot of the alleged 'big data revolution' relates to 'open data' (Kitchin, 2014b, p.xv). In recent years, the government 'appetite' for digital data has intensified (Cate *et al.*, 2012a, p.195). Governments have embraced commercial big data practices under the guise of 'open data initiatives' (Jaatinen, 2016, p.28). The argument for open data follows that increasing government access to digital data as well as the publication of this data on official government websites will improve transparency, decision-making capabilities, innovation opportunities, and public participation (Kitchin, 2014b, pp.55-56). "This idea has led to countless open government data initiatives around the globe"- legitimizing systematic government data collection (Cukier and Mayer-Schonberger, 2013, p.116). As Kuner observes: "The purposes for such data access are highly varied"- including everything from administering taxes and operating national parks to supporting law enforcement and social welfare programs (Kuner, 2013b, p.56). The United States and the European Union are both heavily saturated with private sector businesses and public government initiatives seeking to benefit from big data and open data strategies (Svantesson, 2013, p.285). These emerging practices have heightened the importance of regulatory harmonization between the US and the EU (Weber, 2013, p.130). Specifically, the growing economic value of data collection, storage, and analysis as well as the potentially invasive nature of these activities has put increasing pressure on governments and businesses to develop comprehensive guidelines governing digital data (Cate *et al.*, 2013b, p.65). These tensions, which are interrelated with the development of privacy and data protection as social and legal principles, have become increasingly problematic, not least in the US - EU context (Kuner, 2015a, p.2098).

Security and Surveillance

Beyond narratives about big data and open data, many governments around the world have also embraced digital data for security purposes. Against the background of the 'global war on terror', contemporary governance increasingly entails risk calculation and the use of security practices such as surveillance in order to anticipate security threats (Aradau and Van Munster, 2007, p.91). De Goede characterizes these developments as 'preemptive security governance'- a collection of security practices justified on the basis of risk management (De Goede, 2008, p.164). The convergence between governance, security, and risk has only been magnified by the rise of the Internet and digital technologies (Deibert and Rohozinski, 2010, p.16). In addition to widespread video surveillance, the underlying strategies of preemption have bolstered mass surveillance through the collection of digital data, sometimes referred to as 'dataveillance' (Lyon, 2014, p.4). These practices rely on complex algorithms and software used to process digital data and calculate security risk (Amoore, 2011, p.27). Lyon argues that data-driven surveillance encourages social sorting and predictive profiling, which reverse conventional security practices by placing greater emphasis on prediction and prevention (Lyon, 2014, p.4). Others like Andrejevic and Gates reaffirm that government aspirations for 'total information awareness' necessarily depict every individual as a suspect (Andrejevic and Gates, 2014, p.187). Increasingly, digital data from numerous sources are "abstracted from embodied persons and manipulated to create profiles and risk categories in a networked, rhizomic system" (Lyon, 2002, p.242).

Private sector businesses have taken on a prominent albeit controversial role in contemporary security and surveillance practices. (Ball *et al.*, 2015, p.13). Internet giants like Google, Yahoo, and Microsoft have become increasingly embedded in an emerging 'political economy' of security and surveillance, facilitating government access to digital data (Ball *et al.*, 2015, p.17). Public disclosures made by former US government contractor, Edward Snowden, in May 2013 exposed facets of this complex web of practices- revealing how US government agencies, in tandem with private sector businesses and other government agencies around the world, conduct mass surveillance (Bauman *et al.*, 2014, p.122). The emphasis of the Snowden revelations was placed on surveillance programs operated by the US National Security Agency (NSA), including an integrated online data collection program known as PRISM (Bigo *et al.*, 2013, p.7). The PRISM program was of particular interest given the scope of private sector cooperation with government authorities (Bauman *et al.*, 2014, p.123). These disclosures shed light on complex surveillance networks, blurring the lines between public and private while equally exposing intricate security relationships between different governments around the world (Cate *et al.*, 2013a, p.217).

Within the context of the 'global war on terror', both the United States and the European Union have contributed towards the rise of preemptive security governance and the increasing use of digital data for security and surveillance practices, albeit to varying degrees (Aldrich, 2004, p.731). Notably, the United States has a strong historical legacy of surveillance (Cate, 2008, p.435). The US government adopted the Foreign Intelligence Surveillance Act (FISA) in 1978, authorizing surveillance of foreign subjects without a court order for national security purposes (Bender, 2016, p.120). In the aftermath of the September 11 terror attacks, US Congress enacted the 2001 Patriot Act as an amendment to FISA, enhancing provisions for mass surveillance of both foreign and domestic subjects (Weber, 2013, p.118). In response to growing public concerns about the Snowden revelations, the US government implemented the 2015 Freedom Act to amend FISA and replace the Patriot Act; however, these efforts remain under close national and international scrutiny (Epstein, 2016, p.330).

Since the early 2000s, the European Union has also embraced preemptive security governance, becoming a prominent actor in counterterrorism (Argomaniz *et al.*, 2015, p.196). Security frameworks have gradually embraced mass surveillance and intelligence gathering as central strategies for preventing terrorism- with contributions from EU agencies like Europol and Frontex (Argomaniz *et al.*, 2015, p.200). Den Boer reaffirms: "Intelligence as a process and product has been strongly promoted by the EU as a useful and necessary tool in the fight against terrorism, radicalization, organized crime, and public order problems" (Den Boer, 2015, p.402). Across the EU, these issues have faced controversy. One important example includes the 2006 Data Retention Directive (DRD), which mandated the continued storage of digital data by telecommunications providers across the EU for security purposes (European Parliament, 2006). The Court of Justice of the European Union invalidated the DRD in 2014 on the basis that the scope of data retention disproportionally violated fundamental rights of privacy and data protection (Fabbrini, 2015, p.65). In spite of ongoing controversy, however, EU member states and institutions continue to conduct widespread surveillance for national and regional security purposes (Bigo *et al.*, 2013, p.5).

Adding to these debates, it is important to acknowledge the scope of transatlantic security cooperation and data sharing (Aldrich, 2004, p.731). Following the September 11 terror attacks, the US government called for greater international data sharing to enhance counterterrorism efforts (Kaunert and Léonard, 2013, p.143). While the US government has remained the principal target of public criticism since the Snowden revelations, these issues "cannot be limited to the United States versus the rest of the world" (Bauman *et al.*, 2014, p.121). Indeed, the Snowden revelations also exposed intricate surveillance networks between the US and EU member states like the United Kingdom, the Netherlands, France, Germany, and Sweden (Bauman *et al.*, 2014, p.122). Equally important is the growing role of private sector businesses in transatlantic security and surveillance practices, revealing how "networks of these different services are not only transnational but also hybrids between public and private actors" (Bauman *et al.*, 2014, p.123).

Privacy and Data Protection

A final body of discourses and debates surrounding digital data relates to the development of privacy and data protection as social and legal principles (Kitchin, 2014b, p.168). Privacy is commonly defined as 'being let alone' or 'being free from intrusion', sometimes framed using a discourse of fundamental rights (Langford, 2000, p.65). In the twenty- first century, privacy may be understood as the extension of these values to digital technologies and the Internet (Langford, 2000, p.66). Data protection may be understood as a collection of principles specifically crafted to protect privacy rights in the digital age (Langford, 2000, p.65). There is considerable controversy as to the precise meaning of these concepts (Moulds, 2014, p.16). Some suggest that privacy and data protection are interchangeable terms (Kuner, 2013b, p.20). Others contend that privacy represents American values whereas data protection represents European values (Langford, 2000, pp.65-66). This article will refer to privacy and data protection as a collective phrase, so as to include both sets of vocabularies. It is important to reaffirm, however, that the use of these terms is ongoing and contentious (Bygrave, 2014, p.26).

Above all, privacy and data protection frameworks are created in order to safeguard the "interests and rights of individuals in their role as data subjects- that is, when data about them is processed by others" (Bygrave, 2014, p.1). There is a widespread presumption that privacy and data protection confer positive values onto society and that these values are threatened by the nature of the Internet and digital technologies (Langford, 2000, p.89). However, there is also widespread acceptance of the need to 'balance' these social and legal values with national security interests (Etzioni, 2015, p.104). Given that many governments and businesses around the world address these questions in different ways, there are specific concerns about the need for global harmonization of privacy and data protection as social and legal principles (Bygrave, 2014, p.123). Forums like the United Nations and the Organization for Economic Cooperation and Development have sought to engage with these issues in recent decades; however, there remains no 'universal' approach to privacy and data protection in the twenty-first century (Bygrave, 2014, p.19).

In considering the changing realities of big data and open data as well as security and surveillance practices, it is clear that "none of these concerns fit comfortably within the standard 'privacy-oriented' framing of issues" (Andrejevic, 2014, p.1675). Even so, privacy and data protection frameworks remain the prevailing approach of governments around the world in dealing with questions about the collection, storage, and analysis of digital data. Both the United States and the European Union have historically sought to 'balance' privacy and data protection with security and surveillance while also maximizing the economic value and business incentives of digital data (Cate, 2008, p.482). Despite common objectives, however, major divergences between the United States and the European Union persist (Andrews *et al*., 2005, p.128).

Towards an Analytical Framework

Against this contextual background of digital data, this article will move to consider relevant theoretical contributions across the discipline of International Relations (IR) and beyond. Scholarship from critical data studies and critical security studies will be evaluated in tandem with actor-network theory (ANT) to craft a broad analytical framework. This article does not aspire to present a cohesive theory or methodology but will rather draw upon the notion of 'bricolage'- embracing a multi-disciplinary and multi-method approach in order to more fully grasp the contemporary realities of digital data (Aradau *et al*., 2015, p.7).

Critical Data Studies

Emerging scholarship associated with critical data studies offers nuanced interpretations of the technical and social transformations related to digital data, largely drawing from the disciplines of science and technology studies, geography, and sociology (Kitchin, 2014a, p.7). Without diminishing the diversity of this scholarship, critical data studies may be said to reflect general skepticisms of the 'big data revolution'. As Lupton notes: "A breathless rhetoric has emerged around the concept of big data" (2015, p.94). "Much of the enthusiasm surrounding big data stems from the perception that it offers easy access to massive amounts of data," creating unprecedented business opportunities to monetize this information (Boyd and Crawford, 2012, p.673). Critical data studies scholars such as Strauss seek to 'demystify' these commercial narratives, unpacking the 'seductive power' of big data (Strauss, 2015, p.836). Others like Kitchin are also skeptical of government efforts to adopt big data strategies under the guise of 'open data initiatives', which largely conceals the potentially invasive nature of these activities (Kitchin, 2014b, p.126). Couldry and Powell reaffirm the importance of these critiques, noting: "However misleading or mythical some narratives around big data, the actual processes of data-gathering, data-processing, and organizational adjustment associated with such narratives are not mythical; they constitute an important, if highly contested 'fact', with which all social actors must deal" (Couldry and Powell, 2014, p.1). Kitchin similarly contends that understanding the scope of ongoing transformations related to digital data requires deep knowledge of their technical, temporal-spatial, political, social, and economic implications (Kitchin, 2014b, p.12).

In a broad sense, critical data studies scholarship explores questions of digital data from the 'bottom up' (Couldry and Powell, 2014, p.1). This approach indicates that critical analysis should begin with data itself rather than generic accounts of a 'big data revolution'. In doing so, critical data studies challenges the idea that digital data exist as benign or neutral foundations of modern life, upon which businesses or governments may build (Lupton and Michael, 2015, p.4). Indeed, critical data studies treats digital data "not as static pieces of information, but as participating in a dynamic economy in which they move and circulate" (Lupton, 2015, p.107). In line with these efforts, Lupton observes the tendency across critical data studies to refer to digital data "as living things- as having a kind of organic vitality in their ability to move from site to site, morph into different forms, and possess a 'social life'" (Lupton, 2015, p.108). Relevant contributions include the 'data journeys' framework, which traces the 'life' and movement of digital data across time and space (Bates *et al.*, 2016, p.2). Similar efforts across critical data studies have equally brought attention to "the tendency to overlook the social and cultural lives of data" (Baker *et al.*, 2016, p.2).

Critical data studies also seeks to unpack the complex relationships between humans and digital data- recognizing the agency, reflexivity, and socio-materiality of digital data, in and of itself (Kennedy *et al.*, 2015, p.6). Traditional accounts of digital data tend to obscure its agency, often portrayed as a 'byproduct' of technological advances in the digital age (Lupton, 2015, p.101). Critical data studies moves beyond this one-dimensional view, acknowledging that digital data is a product of human actions and interactions but may equally shape human actions and interactions (Lupton, 2015, p.8). This approach reaffirms the reflexive and circular relationships between humans and digital data, appreciating "how relations between data are also simultaneously relations between people" (Baker *et al.*, 2015, p.131). Building on these understandings of agency and reflexivity, critical data studies also acknowledges the socio- materiality of digital data. On the one hand, the socio-materiality of digital data has a 'physical' manifestation- in computer files, databases, and data storage centers (Bates *et al.*, 2016, p.3). On the other hand, the socio-materiality of digital data has a 'social' manifestation- structuring "our concepts of identity, embodiment, relationship, our choices and preferences, and even our access to services or spaces" (Lupton, 2015, p.26).

While critical data studies offers important contributions upon which this article hopes to build, there are limitations of this scholarship that should be considered. Above all, it is important to reaffirm that critical data studies does not exist in a separate theoretical universe, removed from ongoing developments, but rather "the meaning of critical data studies is as political as the data it engages" (Dalton *et al*., 2016, p.1). Critical data studies also maintains a relatively narrow focus on conceptual and theoretical development, exposing gaps in its empirical contributions (Bates *et al*., 2016, p.2). Adding to these observations, critical data studies remains largely disconnected from many of the security debates that surround digital data, offering limited engagement with questions about the roles of digital data in security practices such as surveillance. In some ways, it may be argued that critical data studies directs significant attention to digital data in everyday life- critiquing private business and public government practices- without considering how these activities also intersect with security practices.

Critical Security Studies

In considering the limitations of critical data studies, critical security studies opens up a unique space to explore the security dimensions of digital data. Within the discipline of International Relations, critical security studies has made meaningful contributions towards the 'broadening' and 'deepening' of security, operating from a consensus that security threats are socially constructed and do not exist a priori (Krause and Williams, 1996, p.230). The critical security studies project encompasses many different 'schools' of thought and the full extent of these academic debates exceeds the scope of this article (Peoples and Vaughan-Williams, 2015, p.9). In recognition of the analytical depth that characterizes critical security studies, it is possible to identify several strands of scholarship that have engaged with questions of digital data, specifically those related to 'surveillance studies' and 'securitization'. Surveillance studies offers meaningful insight into the growing connections between governance, security, and surveillance practices (Balzacq, 2015, p.15). Much of this vast body of literature explores the power relations created by surveillance and relevant ideas surrounding 'governmentality' and the 'panopticon' (Kremer and Müller, 2014, p.8). For the purposes of this article, however, scholarship related to securitization will serve as a primary focus given that it offers more wide- ranging and nuanced approaches to understanding the social construction of (in)security.

Securitization is a broad conceptual framework that has been explored by various schools of critical security studies- with the Copenhagen School representing a foundational approach (McDonald, 2008, p.563). The Copenhagen School embraces the power of language and social interactions, asking who can 'do' or 'speak' security (Buzan *et al*., 1998, p.27). This approach focuses on the discursive constitution of security threats, where referent objects are 'securitized' and shifted from the 'everyday' to the 'exceptional' realm of politics (Buzan *et al*., 1998, p.25). Put another way, securitization may be understood as an intersubjective process where securitizing actors attempt to convince an audience that some object or phenomena poses an existential security threat, warranting a similarly extreme political response (Helgesson and Mörth, 2012, p.4). To 'securitize' is to depict something as 'dangerous', constitutive of an 'existential threat' (Ball *et al*., 2015, p.20). Above all, the securitization framework recognizes that 'security' and 'insecurity' are socially constructed; therefore the characterization and management of security problems cannot be taken for granted (Balzacq *et al*., 2014, p.3). In line with the objectives of this article, securitization facilitates critical analysis about the ways in which digital data may be constructed and reconstructed.

While attention to 'speaking' security has produced meaningful scholarship across critical security studies, significant limitations persist (McDonald, 2008, p.563). Among the criticisms, it is suggested that the Copenhagen School creates binaries between the 'everyday' and the 'exceptional' while also privileging the importance of discourse over materiality (Aradau *et al.*, 2015, p.58). Many of these limitations are evident in the application of securitization to a 'digital' context. As Hansen and Nissenbaum demonstrate, the Copenhagen School approach is not easily applied to the Internet and related digital technologies on the basis of blurred distinctions between 'security' and 'insecurity' as well as the obfuscation of 'speech acts' and 'audiences' in the digital domain (Hansen and Nissenbaum, 2009, p.1157). While Copenhagen School analyses of digital data remain underdeveloped, challenges such as those posed by the Internet and digital technologies are likely to correspond with questions of digital data. On this basis, then, it becomes necessary to consider alternative theorizations of securitization, which build upon and move beyond the Copenhagen School approach.

In response to these shortcomings, productive debates led by scholars such as Balzacq have advanced strands of 'sociological securitization' (Balzacq, 2010, p.1). Moving away from the Copenhagen School tradition, Balzacq recognizes that securitization can be "discursive and non-discursive; intentional and non-intentional" (Balzacq, 2010, p.2). "Security problems can be designed or they can emerge out of different practices, whose initial aim (if they ever had) was not in fact to create a security problem" (Balzacq, 2010, p.2). As Balzacq explains: "Some manifestations of securitization might best be understood by focusing on the nature and functions of policy tools used by agents to cope with public problems, defined as threats" (Balzacq, 2010, p.15). From this perspective, it becomes possible to unpack security threat construction through the critical examination of governance frameworks and policy tools- overcoming the limitations of an exclusively 'discursive' lens (Balzacq, 2008, p.75).

Efforts to carve out space for sociological variants of securitization may also be compatible with calls for the 'materialization' of securitization- or what Aradau describes as attention to "non-human objects in the production of (in)security" (Aradau, 2010, p.509). This approach reinforces the links between material objects, security, and the functioning of everyday life (Aradau, 2010, p.491). In line with these efforts, Salter investigates the role of 'things', considering how the interplay between humans and non-humans compels us to think more critically about security (Salter, 2015, p.vii). While materialism is not new to critical security studies, these contemporary enquiries have brought renewed attention to the relationships between 'discourse' and 'materiality' and between 'humans' and 'non-humans', rather than favoring one over the other (Aradau *et al.*, 2015, p.58). Notable contributions to these efforts include the work of De Goede and Sullivan, who analyze the agency and 'liveliness' of security lists as a critical lens for understanding contemporary security practices and power relations (De Goede and Sullivan, 2015, p.6). Within the context of this article, engagement with materiality and non-human objects in the constitution of (in)security may equally shed light on the 'life' and 'lives' of digital data.

Building on these contributions, Huysmans offers a similarly unconventional approach to 'associative securitization', which highlights the links between securitizing practices through discursive, institutional, and technological forces (Huysmans, 2014, p.83). "This associating will mostly look unspectacular, unexceptional, continuous, and repetitive; instead of speech acts, we get the securitizing 'work' of a multiplicity of little security nothings" (Huysmans, 2011, p.376). Huysmans explores how securitizing processes are 'folded' into everyday life (Huysmans, 2011, p.377). Of particular interest is the diffusion of surveillance in everyday life- referred to as 'extitutional surveillance' (Huysmans, 2016, p.73). Huysmans contends that "the exceptionality of certain surveillance practices…are so thoroughly enveloped in the everyday that it is difficult to maintain the boundary between the two" (Huysmans, 2016, p.79). From this position, security practices can only be understood in their multiplicity (Huysmans, 2016, p.79). These insights help to illuminate the social construction of (in)security as well as the overlapping and contested roles of digital data, which similarly transcend conventional distinctions between the 'everyday' and the 'exceptional'.

Actor-Network Theory

In an attempt to bring together and build upon scholarship from critical data studies and critical security studies, actor-network theory is engaged here as a critical set of tools. Following the contributions of Latour, a leading actor-network theorist, ANT embraces the complex relationships that exist between humans and non-humans (Hassard and Law, 1999, p.4). ANT challenges conventional understandings about non-human objects, resisting the tendency to "take the existence of such objects for granted, as a stable base on which the superstructure of international politics is subsequently erected" (Barry, 2013, p.421). Latour reaffirms: "It is a theory, and a strong one, but about how to study things, or rather how not to study them" (Latour, 2005, p.142). Above all, ANT is driven by the mutually constitutive and fluid relationships that exist between human and non-human actors, which are envisioned as 'networks' (Nexon and Pouliot, 2013, p.343). Latour clarifies this point, noting: "It is in this complete reversibility- an actor is nothing but a network, except that a network is nothing but actors" (Latour, 2011, p.800).

Another important contribution of ANT relates to 'assemblage thinking' and the ability to map heterogeneous relations and associations (Müller, 2015, p.28). Müller explores the links between actor-network theory and assemblage thinking, observing that: "Both are concerned with why orders emerge in particular ways, how they hold together, somewhat precariously, how they reach across or mold space, and how they fall apart" (Müller, 2015, p.27). From a corresponding position, Law and Singleton argue that ANT is well equipped to deal with multiplicity and heterogeneity (Law and Singleton, 2014, p.379). "The crucial point is since there are lots of practices there are also multiple realities. Practices are sitting alongside one another in different places and practices, and what becomes really important is how the different…realities get related together in practice" (Law and Singleton, 2014, p.386). Ultimately, actor-network theory and assemblage thinking demonstrate a strong capacity to make sense of multiple human and nonhuman actors as well as multiple discourses and practices.

For the purposes of this article, bringing ANT into a 'digital' context has meaningful implications that should be considered. Latour acknowledges the opportunities and challenges related to this transition, noting the capacity of ANT to move beyond conventional distinctions between the 'digital' world and the 'real' world, thus allowing for more fluid conceptualizations of contemporary socio-material relations (Latour, 2011, p.809). Lupton elaborates on this potential, observing that: "In emphasizing the role of agency and non-human actors in shaping human actors…exponents contend that humans are always imbricated within networks comprised of human and non-human actors and cannot be isolated from these networks" (Lupton, 2015, p.23). While theoretical engagement with ANT in the context of digital data remains limited, scholars such as Michael reiterate the broader importance of understanding "how the 'digital' is part of the 'social' and vice versa" (Michael, 2017, p.149).

In determining the relevance of ANT to this analytical framework, there are limitationsthat must also be addressed. Müller reminds us that actor-network theory and assemblage thinking have found a 'cautious reception' within the discipline of International Relations (Müller, 2015, p.27). As Barry contends: "Actor-network theory thrives on details and fragments of evidence, which are never likely to add up to a complete picture but will nonetheless reveal something that was perhaps unexpected or unanticipated" (Barry, 2013, p.418). Nexon and Pouliot similarly argue that the emphasis on 'uncertainty' and 'fluidity' within ANT literature may inhibit empirical investigations (Nexon and Pouliot, 2013, p.344). From this position, ANT "cannot be simply applied as a theory," but rather demands a complete reconfiguration of research questions and methodologies (Barry, 2013, p.414). In spite of these potential obstacles, ANT may be used to reimagine traditional tensions and debates across International Relations (Nexon and Pouliot, 2013, p.345). Here, it is useful to return to Latour's claim that ANT is a theory "about how to study things, or rather, how not to study them" (Latour, 2005, p.142).

'Bricolage' in Context

This article brings together an eclectic combination of scholarship, operating from the position that each body of literature has something to offer the other. The objectives of this article ultimately reinforce multi-disciplinary and multi-method engagement (Aradau *et al.*, 2015, p.7). Such an approach moves away from 'rigid' epistemological and methodological choices within the discipline of IR- echoing a growing acceptance of 'bricolage' and the benefits of "experimenting with combining theories, concepts, [and] methods" (Aradau *et al.*, 2015, p.8). In considering the task of constructing an analytical framework, critical data studies and critical security studies provide important starting points for this investigation. Actor- network theory and assemblage thinking become vehicles to engage with the concepts that exceed the scope of both critical data studies and critical security studies. Following the example of 'bricolage', it is useful to briefly summarize how these diverse strands of scholarship come together and build upon one another.

Critical data studies seeks to unpack the narratives and practices surrounding the 'big data revolution', producing a variety of conceptual and theoretical frameworks that reassert the power of digital data, in and of itself. Above all, critical data studies reiterates the importance of analyzing the agency, mobility, socio-materiality, and 'liveliness' of digital data in the contemporary world. In spite of these contributions, however, critical data studies remains broadly disconnected from ongoing security debates. In some ways, it may be argued that critical data studies directs attention to digital data in ordinary business and government practices without considering the overlapping and contested roles of digital data in extraordinary security practices. Critical data studies would be strengthened by empirical development and greater attention to the ways in which digital data can occupy the space between the 'everyday' and the 'exceptional'.

Critical security studies and the securitization framework provide meaningful insights into the social construction of security and insecurity, addressing some of the aforementioned 'gaps' in critical data studies. This article will primarily draw upon the contributions of Balzacq's 'sociological securitization' and Huysmans' 'associative securitization', which highlight the web of agents, practices, and policies surrounding the construction of (in)security as well as the interlinking roles of human and non-human actors. Balzacq and Huysmans collectively reaffirm that securitization embodies a set of ongoing and performative processes that may take diverse forms. This is particularly useful in considering how digital data may be framed as a 'security threat' while simultaneously being framed as part of a 'security-enhancing' strategy through practices such as surveillance. Huysmans also reaffirms the importance of understanding how 'mundane' objects and practices become embedded within these processes. For the purposes of this article, then, securitization enables us to conceptualize how referent objects move between the 'everyday' and the 'exceptional'. Going beyond this, however, sociological strands of securitization begin to shed light on how these distinctions are messy, blurred, and overlapping.

ANT and assemblage thinking provide important conceptual channels across critical data studies and critical security studies. On the one hand, ANT echoes critical data studies, treating digital data as a socio-material object with agency and reflexivity. Assemblage thinking likewise embraces the complex ways that humans and non-human actors interact (Lupton, 2015, p.24). On the other hand, ANT and assemblage thinking bolster critical security studies and securitization. ANT reinforces renewed attention to materiality and the roles of human and nonhuman actors in the constitution of (in)security. In recent years, critical security studies has gradually opened up to ANT and assemblage thinking. Notable efforts include those of Balzacq and Dunn-Cavelty, who explore ANT in tandem with securitization in order to analyze cybersecurity threats (Balzacq and Dunn-Cavelty, 2012, p.197). Huysmans, too, proposes that the 'assemblage' offers a useful conceptual tool for analyzing the diffusion of (in)security (Huysmans, 2014, p.108). ANT and assemblage thinking strengthen the conceptualization of these processes in their fluidity and their reflexivity.

For the purposes of this article, digital data is positioned as a non-human actor with agency, mobility, and socio-materiality- actively shaping and being shaped by human actions and interactions. The narratives and practices surrounding digital data are fluid, heterogeneous, and intersubjective. From this position, there are multiple human and nonhuman actors that come into play- bringing together a complex assemblage of consumers, private businesses, government agencies, regulatory bodies, data intermediaries, data storage centers, and digital data itself. This investigation builds from an understanding that different actors can use and reuse digital data in different ways or in the same ways more than once. Not only can digital data be generated and collected but digital data can also be shared, repurposed, recontextualized, aggregated, or disaggregated. Returning to the driving research questions of this article, it is argued that digital data may be simultaneously constructed as a 'mundane' feature of everyday life, as a component of 'security-enhancing' strategies, and as a 'security threat'. This article also recognizes that digital data may wield socio-material power over human actors, taking on a 'liveliness' of its own.

Building on this analytical orientation, the US - EU Safe Harbor Framework will be evaluated as an empirical case study to demonstrate how digital data may be constructed in overlapping and contested ways. Rather than exploring the Safe Harbor Framework as a singular or static phenomenon, this article appreciates the ongoing changes and processes that characterize its development and deterioration. This approach reinforces the claims that securitization can occur through "the functions and implications of policy tools used to meet a public problem" (Balzacq, 2008, p.75). This analytical framework also embraces the importance of evaluating social and political processes "that may not be visibly associated with securitization but that may supply important parts of the jigsaw puzzle" (Helgesson and Mörth, 2012, p.6).

Case Study: The US - EU Safe Harbor Framework

The United States and the European Union manage the collection, storage, and analysis of digital data in distinctive ways (Langford, 2000, p.87). While the US is commonly critiqued for its failure to present a cohesive framework to govern digital data, the EU has, on the contrary, faced criticism for its 'overreach' (Svantesson, 2013, p.286). Historically, the US has favored a decentralized approach, relying on voluntary mechanisms and guidelines developed by the private sector for collecting, storing, and analyzing digital data (Shimanek, 2001, p.472). Notably, "there is no general framework covering every sector, creating general rights [and] obligations" (Andrews *et al.*, 2005, p.116). In contrast, the EU has crafted a comprehensive legal and regulatory agenda around digital data (Shimanek, 2001, p.472). The foundation of the European approach is the 1995 Data Protection Directive (DPD) (European Parliament, 2006). The DPD upholds data protection as a fundamental right extended to all citizens of the EU- establishing Data Protection Authorities as supervisory bodies in every member state and determining appropriate conditions for collecting and storing digital data generated in the EU (European Parliament, 1995). Drawing from a legal tradition that views data protection as a fundamental right, the DPD is reinforced by provisions in the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights (Fundamental Rights Agency, 2014, p.14). The CJEU has also demonstrated considerable engagement with questions of privacy and data protection in recent years. There is an extensive body of relevant case law, much of which exceeds the scope of this article (Laudati, 2015, p.1). However, it is important to acknowledge several landmark cases overseen by the CJEU, including *Digital Rights Ireland* and *Google Spain*- both of which strengthened the European position on data protection as a fundamental right (Ni Loidean, 2016, p.11).

With regards to processing and transferring digital data outside the EU, the European approach is primarily based on 'adequacy principles' (Kuner, 2013b, p.76). Under the DPD, "transborder data flows are not allowed unless the recipient country provides an adequate level of protection as determined by the European Commission" (Weber, 2013, p.120). "In essence, the adequacy requirement is a mechanism to ensure that there are no loopholes found in the high level of protection of personal data provided by the [DPD]" (De Hert *et al.*, 2016, p.27). Over time, EU adequacy principles have gained global significance, shaping the development of privacy and data protection frameworks around the world to satisfy European preferences (Kuner, 2013b, p.106). There is an increasing assumption that EU data protection frameworks have an 'extraterritorial scope', thereby extending protections for EU citizens to all locations where digital data is transferred (Kuner, 2015b, p.243). These arguments surrounding European regulatory overreach and extraterritoriality remain controversial, not least in the transatlantic context (Kong, 2010, p.441).

The Safe Harbor Framework was created by US and EU policymakers in July 2000 to 'bridge' the transatlantic divide in privacy and data protection- providing for "the systemic and free flow of data from the EU without any conflicts arising under the Data Protection Directive" (De Hert *et al.*, 2016, p.27). Given that the US did not meet the requirements of the DPD, the notion of a 'safe harbor' suggested it was possible to craft adequacy protections through a set of established guidelines, jointly enforced by US and EU authorities (Kuner, 2013b, p.125). These guidelines would be known as the 'Safe Harbor principles', including: notice, choice, consent, onward transfer, data integrity, access, and enforcement (European Commission, 2000). Under the Safe Harbor Framework, US businesses could voluntarily register for Safe Harbor certification, thereby accepting a legal obligation to uphold the Safe Harbor principles in exchange for adequacy status in the EU (Shimanek, 2001, p.473).

From its inception, the Safe Harbor Framework was not viewed "as an overwhelming success on either side of the Atlantic" (Kobrin, 2004, p.121). Many contended that the very logic of 'safe harbors' was flawed, combining US preferences for self-regulation with robust social and legal mechanisms for privacy and data protection in the EU (Colonna, 2014, p.203). As Regan observes: "Under the thin veil of the Safe Harbor principles...there is no one government entity but fragmented state and local agencies with sometimes unclear jurisdictions" (Regan, 2003, p.275). Clunan and Trinkunas also note that "the EU was the agenda setter and enforced compliance," creating particular tensions with the US (Clunan and Trikunas, 2010, p.244). Ongoing transformations in the twenty-first century have only intensified these strains on the Safe Harbor principles, specifically related to the increasing collection and processing of digital data by businesses and governments (Kuner, 2009, p.2). In the contemporary world, "data are not just transferred once and then locked away," but are rather used and reused by a variety of actors in disclosed and undisclosed ways (Kuner, 2009, p.1). These tensions were exacerbated by the Snowden revelations about US government surveillance, which began to unfold in May 2013 (Farrell and Newman, 2016, p.130). In response, the European Commission called for a broad reexamination of the Safe Harbor principles; however, significant concerns persisted across the EU (De Hert *et al.*, 2016, p.30).

The viability of the Safe Harbor Framework began to unravel when an Austrian citizen- Maximillian Schrems- filed a complaint in June 2013 with the Irish Data Protection Commissioner against the US social media company, Facebook, whose European headquarters are located in Ireland. Schrems claimed that Facebook was actively violating "his data protection rights by transferring his personal data to the [United States] and the US security services were accessing that data" (Fitzgerald, 2016, p.9). This complaint was later referred to the CJEU, where the Court held that the US was in breach of the fundamental rights of EU citizens, ultimately invalidating the Safe Harbor Framework in October 2015. This judgment, known as the Schrems Decision, created significant distress across the Atlantic, jeopardizing digital data flows between the EU and the US (Tracol, 2016, p.345). While the Schrems Decision was hailed as a triumph for fundamental rights in the EU, the sudden deterioration of the Safe Harbor Framework was both unexpected and unwelcome in the US (Epstein, 2016, p.337). Interestingly, the CJEU did not exclusively focus on Facebook but rather extended the scope of its judgment to thousands of Safe Harbor-certified companies (Tracol, 2016, p.358). Determann also observes that the CJEU "did not address these topics in any depth but merely referred to the vague assertions of the complainant in the Irish proceedings as well as media reports about NSA espionage, without establishing a comparative context to...similar surveillance activities" across the European Union (Determann, 2016, p.245).

The development and deterioration of the US - EU Safe Harbor Framework illuminates the diverging ways in which digital data are constructed and reconstructed in the contemporary world. Between July 2000 and October 2015, various actors attempted to frame digital data as posing an existential 'security threat' while simultaneously justifying the same or related practices involving digital data as 'mundane' features of everyday life or as part of broader 'security-enhancing' strategies. The following sections will mobilize the analytical framework set forth in this article to unpack these overlapping and contested roles- drawing on critical data studies, critical security studies, and actor-network theory to appreciate the agency, mobility, and socio-material power of digital data as well as the complex relationships between human and non-human actors in the constitution of (in)security.

In evaluating the Safe Harbor Framework through the analytical approach set forth in this article, it is important to acknowledge that there are multiple 'agents' and 'audiences' of securitization (Helgesson and Mörth, 2012, p.132). The primary agents of securitization are public government and private business actors involved in the development and deterioration of this governance arrangement- namely, the US Federal Trade Commission, the US Department of Commerce, the European Commission, the European Parliament, Data Protection Authorities, and the Court of Justice of the European Union as well as US-based private sector industries with interests in facilitating transatlantic data flows. The primary audiences are broadly comprised of public citizens across the US and the EU; however, these audiences are neither 'passive' nor can they be considered inherently 'compatible' (Balzacq, 2010, p.9).

Going further, this proposes that digital data is 'alive' and has many 'lives'. On this basis, digital data becomes an agent within the securitization framework- reaffirming that digital data is not only a material 'thing' that exists in the contemporary world (Turner, 2009, p.154). Here, ANT and assemblage thinking help to make sense of these complex 'networks' of human and non-human actors that are constructing digital data in overlapping and contested ways. Helgesson and Mörth suggest that this multiplicity of agents and audiences raises an important question: "Where does one draw the line concerning who is responsible for what aspects of the securitization process?" (Helgesson and Mörth, 2012, p.6). Accordingly, this analytical approach appreciates how changing relationships between securitizing actors, audiences, and referent objects reflect the nature of securitization as an intersubjective process.

Digital Data as 'Mundane'

The Safe Harbor Framework was developed, first and foremost, in response to the awareness that the US did not meet the adequacy principles of the EU Data Protection Directive (Weber, 2013, p.126). The negotiation of the Safe Harbor Framework was also broadly linked with efforts to create a 'digital marketplace' for transatlantic commerce, recognizing the growing economic value of digital data (Andrews *et al*., 2005, p.101). Notably, the principles underlying the Safe Harbor Framework were crafted prior to the advent of big data practices and technologies (Cate *et al*., 2012b, p.47). The Safe Harbor Framework was also conceptualized before the upsurge of preemptive security and narratives about the global war on terror (Bellanova, 2014, p.112). From this position, digital data was framed as the product of everyday activities, like emailing and web browsing. Equally, the collection of digital data by private sector industries was framed as part of routine procedures, which enhanced business operations (Ball *et al*., 2015, p.22). As Huysmans reaffirms: "In itself, data gathering is not connected to the diffusing of insecurities" (Huysmans, 2014, p.97). On this basis, the development of the Safe Harbor Framework constructed digital data neither as part of 'security-enhancing' practices nor as a 'threat' to individuals and society. Rather, the development of the Safe Harbor Framework presented digital data as a 'mundane' feature of everyday life.

Digital Data as 'Security-Enhancing'

As the twenty-first century progressed, the Safe Harbor Framework was made to coexist alongside mounting questions about the importance of data collection and data sharing for security purposes in the United States and the European Union. With the rise of preemptive security and risk-based governance that accompanied the global war on terror, digital data was increasingly constructed as part of security-enhancing strategies on both sides of the Atlantic (Weber, 2013, p.118). As a consequence, the collection of digital data for security and surveillance purposes was framed as "necessary for the protection and defense of democracy, fundamental rights, and freedoms of citizens" (Barnard-Wills, 2013, p.172). These potentially invasive activities- which involved both public government and private business actors- were broadly legitimized on the basis of the 'common good' (Etzioni, 2015, p.104). The Safe Harbor principles were not altered to reflect ongoing transformations in the nature of security and surveillance or the 'boundary blurring' of public-private actors in the security domain (Helgesson and Mörth, 2012, p.132). Instead, digital data was framed as a component of 'security-enhancing' strategies, subsequently used by actors to 'securitize' other referent objects.

Digital Data as a 'Security Threat'

As the twenty-first century unfolded, competing pressures surrounding digital data continued to intensify. Within the context of the Snowden revelations and the Schrems Decision, the acquisition of digital data by US government agencies like the NSA was framed by the CJEU as posing a security threat to the claimant, Maximillian Schrems, and all other citizens of the European Union. Put another way, digital data was securitized on the basis that the widespread collection of digital data in the US infringed upon the fundamental rights of EU citizens (Fabbrini, 2015, p.65). This perception of digital data as a security threat relates to concerns about the invasive nature of data-driven surveillance practices like social sorting and predictive profiling- where "states and corporations know and anticipate so much about individuals…that they possess the power to enforce rigid and pernicious forms of disciplinary control" (Kitchin, 2014b, p.180). As Poulin concedes: "The actions of large corporations…and governments have the potential to affect behavioral change on those populations" (Poulin, 2014, p.113). Amoore goes further, arguing: "The harm is in the violence done to associational life, to the potentiality of futures that are as yet unknowable" (Amoore, 2014, p.110). This has been referred to elsewhere as 'digital footprints' and 'digital shadows'- signaling that the nature of threats posed by digital data is multilayered and, at times, unknown (Koops, 2011, p.1). In different ways, then, the deterioration of the Safe Harbor Framework constructed digital data as a dangerous 'security threat' to individuals and society.

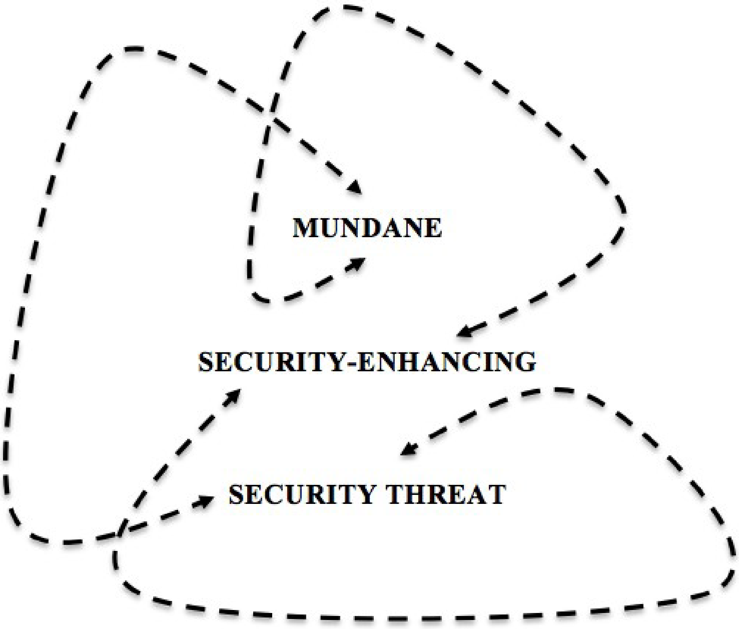

Figure A Overlapping and Contested Roles of Digital Data

Crucial to this analysis is the recognition that these different roles of digital data are overlapping and contested (see Figure A)- creating a complex assemblage of relations (Aradau and Blanke, 2015, p.1). This assemblage may be disentangled in the following ways: Consumers willingly contribute vast amounts of information through actions and interactions online, generating huge amounts of digital data that can be aggregated, stored, and analyzed to produce insights about various social behaviors (Galič *et al.*, 2016, p.21). Private sector industries collect this digital data on the basis of broad consumer consent (Lupton, 2015, p.37). Government agencies also collect this digital data on the more limited basis of national security and governance purposes. Adding to these phenomena, many private sector businesses are voluntarily or involuntarily cooperating with government agencies to provide access to the vast amount of digital data in their possession (Cate *et al.*, 2013a, p.218). What becomes clear is that: "Today, threats...emerge in a highly connected and technologically complex world where a myriad of public and private actors participate, perhaps even unwittingly, in creating them" (De Hert *et al.*, 2016, p.25). In this way, the same digital data generated and collected through 'mundane' practices may become an existential 'security threat' or a broader component of 'security-enhancing' strategies.

This analysis suggests that digital data may be simultaneously constitutive of 'security' and 'insecurity'. But how is it possible that digital data can be constructed and reconstructed in these multiple and sometimes contradictory ways? In order to make sense of these overlapping and contested roles, this article has proposed that digital data is 'alive' and has many 'lives'. Reconceptualizing digital data in this way allows for greater insight into the nature of digital data in the contemporary world. Once digital data is generated, this information may continue to move and transform, "disconnected from the continuing embodied experience of the individuals from which they were extracted" (Huysmans, 2014, p.99). In some ways, this conceptualization of the 'liveliness' of digital data is compatible with what Lyon refers to as 'data doubles'- signaling the duality between an individual and the information generated by that individual, which may go on to circulate in known and unknown ways (Lyon, 2006, p.77). However, this approach goes one step further, opening up the possibility that digital data may become a securitizing actor, in and of itself.

Bringing these strands together, this case study analysis concludes that it is possible to understand how digital data may be constructed in overlapping and contested ways when it is acknowledged that digital data is 'alive' and has many 'lives'. In considering these factors within the context of the US - EU Safe Harbor Framework, it may be argued that digital data is not only 'securitized' as an existential threat and used by different actors to 'securitize' other referent objects but digital data itself may also become an agent of securitization. The Safe Harbor Framework did not adequately address this 'liveliness', which ultimately helps to explain why this governance arrangement failed to withstand emerging pressures related to digital data. Embracing the notion that digital data possesses agency, mobility, and socio-material power makes it possible to engage more critically with contemporary realities and redress the ways in which digital data are conceptualized in the twenty-first century.

Beyond Safe Harbors

While the Safe Harbor Framework remains central to this analysis, there have been several legal and regulatory developments since its invalidation in October 2015. The US and the EU came together in February 2016 to negotiate a new adequacy agreement- the Privacy Shield- as a successor to the Safe Harbor Framework (European Commission, 2016). The Privacy Shield introduces new mechanisms for transatlantic cooperation; however, much of its content remains closely aligned with the original Safe Harbor Framework (Bender, 2016, p.130). The EU also introduced the General Data Protection Regulation (GDPR) as an updated framework to replace the DPD (European Parliament, 2016). The GDPR, which went into effect in May 2018, builds on the legacy of the DPD while equally advancing stronger protections for individuals (Van der Sloot, 2014, p.315). In the European Union, the Brexit referendum and subsequent negotiations have created "particular uncertainty regarding the fate of the EU's GDPR in the United Kingdom" given that "Brexit will again put the spotlight on the EU's criterion of adequacy for data transfers" (Cate *et al.*, 2016, p.167). Others have pointed to concerns about the election of US

President Donald Trump, who has yet to directly address issues of privacy and data protection between the United States and the European Union (McDermott, 2017, p.4).

Adding to these challenges, a second legal case was launched in June 2016 against Facebook in the European Union, known widely as 'Schrems II' (Cate *et al.*, 2016, p.168). Similar to its predecessor, this case challenges provisions for 'standard contractual clauses' within adequacy frameworks like the Privacy Shield, which permit transfers of digital data outside of the EU on a contract basis (Fitzgerald, 2016, p.9). While the invalidation of the Safe Harbor Framework had significant consequences in the transatlantic context, Schrems II challenges the use of standard contractual clauses on a more global scope- threatening adequacy decisions around the world as well as undermining the legal basis of adequacy itself (Fitzgerald, 2016, p.11). For these reasons, Schrems II has been described as "one of the most important cases that the [CJEU] will ever hear" (Fitzgerald, 2016, p.11). At the time of writing, these legal proceedings are ongoing.

In considering these unfolding developments, what is the way forward? And must there only be one path? Tene argues "the new generation of technology and of users calls for a new generation of data protection" (Tene, 2011, p.16). Others, like Koops, are less optimistic about the future of governance arrangements like the Safe Harbor Framework in the digital age (Koops, 2014, p.250). Kuner, too, concedes: "The search for an overarching solution may in itself be problematic, since it can give rise to unrealistic expectations" (Kuner, 2013b, p.186). No single policy or set of principles can "wholly resolve these tensions, since they reflect the hypocrisies of a world simultaneously fascinated by the benefits of globalization and of the Internet and frightened by the insecurities they bring" (Kuner, 2013b, p.187).

Ultimately, it remains unproductive to rely on governance arrangements such as the Safe Harbor Framework to address emerging challenges of digital data in the US - EU context and beyond. Until governance frameworks embrace the tensions of the overlapping and contested roles of digital data, they are unlikely to sustain contemporary pressures from unfolding discourses and debates like those surrounding big data and open data, security and surveillance, as well as privacy and data protection. This was clearly demonstrated by the deterioration of the Safe Harbor Framework as well as ongoing uncertainties about the viability of the Privacy Shield. Looking ahead, alternative approaches are needed in order to account for the 'liveliness' of digital data in the contemporary world- repositioning digital data as a non-human actor with agency, mobility, reflexivity, and socio-material power.

Conclusions

This article has sought to disentangle the fragmented and competing discourses and practices that come together in an assemblage of 'digital data'. The development and deterioration of the US - EU Safe Harbor Framework illustrated how digital data may be constructed in overlapping and contested ways- simultaneously framed as a mundane feature of everyday life, as a component of security-enhancing strategies as well as an existential security threat. In order to make sense of this fluidity and multiplicity, this article proposed that digital data is 'alive' and has many 'lives'- reconceptualizing how digital data is actively shaping and being shaped by the contemporary world.

Digital data has been engaged across the discipline of IR in different ways, however, this article has sought to 'fill the gaps'- advancing the critical study of digital data through a security-focused lens. The spirit of this research reflects an ambition to understand the fullest spectrum possible of ways in which digital data is constructing and being constructed. The scope of this research was necessarily limited to focus on several major discourses and debates surrounding digital data in the context of the United States and the European Union, namely: big data and open data, security and surveillance, and privacy and data protection. It is acknowledged, however, that these categories are largely arbitrary and many of these discourses and debates are still unfolding. Additionally, in considering potential limitations surrounding the empirical case study evaluated, it is important to reaffirm that the US - EU Safe Harbor Framework is not, in its intention, a 'security-driven' policy tool. However, much of the scholarship surrounding the Safe Harbor Framework remains entrenched in dense legal debates, without critical attention to the roles of digital data in security contexts or the changing realities of business and governance practices. This sense of discord reinforces the need to evaluate the Safe Harbor Framework through a security lens- offering a unique entry point to exploring digital data as a multilayered and performative process.

Contemporary society continues to grapple with new realities of digital data in the twenty-first century- increasingly dominated by business efforts to monetize digital data, government efforts to remediate digital data for various governance and security purposes as well as social and political efforts to confer distinctive rights and obligations onto the subjects and controllers of digital data. Not only are these phenomena parallel, they are also perpendicular- intersecting in complex and multidimensional ways. Governance arrangements such as the Safe Harbor Framework remain the dominant approach for managing digital data flows in the contemporary world but they need not be the only approach. Ultimately, the ways that governments, businesses, and individuals around the world choose to navigate the challenges of digital data will serve as a reflection of broader global tensions and priorities (Kuner, 2013b, p.18). For these reasons, digital data must be critically engaged and reimagined in ways that more powerfully capture the dynamics of an increasingly 'datafied' world.

About the author

Katarina Rebello graduated from the University of St Andrews with a degree in International Relations. Her primary interests fall at the intersection of politics, policy, and technology innovation, with particular attention to the transatlantic community. She is a dual US – EU citizen, currently working at a technology policy research and advocacy organization based in Washington DC. In this role, she works closely with government agencies, businesses, nonprofit organizations, and multilateral organizations like the United Nations and the World Bank to develop data policies.

Bibliography

Aiden, Erez and Michel, Jean-Baptiste (2013) *Uncharted: Big Data as a Lens on Human Culture*, New York, USA: Riverhead Books.

Aldrich, Richard (2004) 'Transatlantic Intelligence and Security Cooperation', *International Affairs*, 80(4), pp. 731-753.

Amoore, Louise (2011) 'Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times', *Theory, Culture & Society*, 28(6), pp. 24-43.

Amoore, Louise (2014) 'Security and the Claim to Privacy', *International Political Sociology*, 8(1), pp. 108-112.

Andrejevic, Mark and Gates, Kelly (2014) 'Big Data Surveillance', *Surveillance and Society*, 12(2), 185-196.

Andrejevic, Mark (2014) 'The Big Data Divide', *International Journal of Communication*, 8(0), pp. 1673-1689.

Andrews, David, Pollack, Mark, Shaffer, Gregory, and Wallace, Helen (2005) *The Future of Transatlantic Economic Relations: Continuity Amid Discord*, Florence, Italy: Robert Schuman Center for Advanced Studies.

Aradau, Claudia, Huysmans, Jef, Neal, Andrew, and Voelkner, Nadine (2015) *Critical Security Methods: New Frameworks for Analysis*, Abingdon, UK: Routledge.

Aradau, Claudia and Van Munster, Rens (2007) 'Governing Through Risk: Taking Precautions, (Un) Knowing the Future', *European Journal of International Relations*, 13(1), pp. 89- 115.

Aradau, Claudia (2010) 'Security That Matters: Critical Infrastructure and Objects of Protection', *Security Dialogue*, 41(5), pp. 491-514.

Aradau, Claudia and Blanke, Tobias (2015) 'The (Big) Data Security Assemblage: Knowledge And Critique', *Big Data & Society*, 2(1), pp. 1-12.

Argomaniz, Javier, Bures, Oldrich and Kaunert, Christian (2015) 'A Decade of EU Counterterrorism and Intelligence: A Critical Assessment', *Intelligence and National Security*, 30(2-3), pp. 191-206.

Baker, Stephanie A., Harvey, Penny, Kallianos, Yannis, Lewis, Camilla, Lury, Celia, McNally, Ruth, and Ruppert, Evelyn (2015) 'Socializing Big Data: From Concept to Practice', *CRESC Working Paper*, 138(0), pp. 1-48.

Ball, Kirstie, Canhoto, Ana, Daniel, Elizabeth, Dibb, Sally, Meadows, Maureen, and Spiller, Keith (2015) *The Private Security State? Surveillance, Consumer Data, and the War on Terror*, Copenhagen, Denmark: CBS Press.

Balzacq, Thierry and Dunn-Cavelty, Myriam (2012) 'Actor-Network Theory of Cyber- Security', *European Journal of International Security*, 1(2), pp. 176-198.

Balzacq, Thierry (2015) Contesting Security: Strategies and Logics, London, UK: Routledge. Balzacq, Thierry (2010) *Securitization Theory: How Security Problems Emerge and Dissolve*, Abingdon, UK: Routledge.

Balzacq, Thierry (2008) 'The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies', *Journal of Common Market Studies*, 46(1), pp. 75-100.

Balzacq, Thierry, Guzzini, Stefano, Patomäki, Heikki, Waever, Ole, and Williams, Michael (2014) 'What Kind of Theory- If Any- Is Securitization?', *International Relations*, 29(1), pp. 1-41.

Barnard-Wills, David (2013) 'Security, Privacy, and Surveillance in European Policy Documents', *International Data Privacy Law*, 3(3), pp. 170-180.

Barry, Andrew (2013) 'The Translation Zone: Between Actor-Network Theory and International Relations', *Millennium Journal of International Studies*, 41(3), pp. 413-429.

Bates, Jo, Goodale, Paula, and Lin, Yu-Wei (2016) 'Data Journeys: Capturing the Socio- Material Constitution of Data Objects and Flows', *Big Data & Society*, 3(2), pp. 1-12.

Bauman, Zygmunt, Bigo, Didier, Esteves, Paulo, Guild, Elspeth, Jabri, Vivienne, Lyon, David, and Walker, R. B. J. (2014) 'After Snowden: Rethinking the Impact of Surveillance', *International Political Sociology*, 8(2), pp. 121-144.

Bellanova, Rocco (2014) 'Data Protection, With Love'. *International Political Sociology*, 8(1), pp. 112-115.

Bender, David (2016) 'Having Mishandled Safe Harbor, Will the CJEU Do Better With Privacy Shield? A US Perspective', *International Data Privacy Law*, 6(2), pp. 117-138.

Bigo, Didier, Carrera, Sergio, Hernanz, Nicholas, Jeandesboz, Julien, Parkin, Joanna, Ragazzi, Francesco, and Scherrer, Amandine (2013) *National Programs for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law*, Brussels, Belgium: European Union.

Boyd, Danah and Crawford, Kate (2012) 'Critical Questions for Big Data: Provocations For a Cultural, Technological, and Scholarly Phenomenon', *Information, Communication & Society*, 15(5), pp. 662-679.

Buzan, Barry, Waever, Ole, and de Wilde, Jaap (1998) *Security: A New Framework for Analysis*, London, UK: Lynne Rienner Publishers.

Bygrave, Lee Andrew (2014) *Data Privacy Law: An International Perspective*, Oxford, UK: Oxford University Press.

Cate, Fred (2008) 'Government Data Mining: The Need for a Legal Framework', *Harvard Civil Rights Civil Liberties Law Review*, 43(2), pp. 435-489.

Cate, Fred, Dempsey, James, and Rubinstein, Ira S. (2012a) 'Systematic Government Access to Private-Sector Data', *International Data Privacy Law*, 2(4), pp. 195-199.

Cate, Fred, Kuner, Christopher, Millard, Christopher, and Svantesson, Dan Jerker B. (2012b) 'The Challenge of Big Data for Data Protection', *International Data Privacy Law*, 2(2), pp. 47-49.

Cate, Fred, Kuner, Christopher, Millard, Christopher, and Svantesson, Dan Jerker B. (2013a) 'PRISM and Privacy: Will This Change Everything?' *International Data Privacy Law*, 3(4), pp. 217-219.

Cate, Fred, Kuner, Christopher, Millard, Christopher, and Svantesson, Dan Jerker B. (2013b) 'The Business of Privacy', *International Data Privacy Law*, 3(2), pp. 65-66.

Cate, Fred, Kuner, Christopher, Lynskey, Orla, Millard, Christopher, and Svantesson, Dan Jerker (2016) 'The Global Data Protection Implications of Brexit', *International Data Protection Law*, 6(3), pp. 167-169.

Clunan, Anne and Trinkunas, Harold (2010) *Ungoverned Spaces: Alternatives to State Authority in an Era of Softened Sovereignty*, Stanford, USA: Stanford University Press.

Colonna, Liane (2014) 'Article 4 of the EU Data Protection Directive and the Irrelevance of the EU-US Safe Harbor Program', *International Data Privacy Law*, 4(3), pp. 203-221.

Connolly, Chris (2008) The US Safe Harbor: Fact or Fiction? Sydney, Australia: Galexia Ltd. Couldry, Nick and Powell, Alison (2014) 'Big Data from the Bottom Up', *Big Data and Society*, 1(1), pp. 1-5.

Court of Justice of the European Union (2015) *Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner*, 6 October 2015, Available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf (Accessed 22 March 2016).

Cukier, Kenneth and Mayer-Schonberger, Viktor (2013) *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, London, UK: John Murray Publishers.

Custers, Bart and Ursic, Helena (2016) 'Big Data and Data Reuse: A Taxonomy of Data Reuse For Balancing Big Data Benefits and Personal Data Protection', *International Data Privacy Law*, 6(1), pp. 4-15.

Dalton, Craig, Taylor, Linnet, and Thatcher, Jim (2016) 'Critical Data Studies: A Dialogue on Data and Space', *Big Data and Society*, 3(1), pp. 1-9.

De Goede, Marieke (2008) 'The Politics of Preemption and the War on Terror in Europe', *European Journal of International Relations*, 14(1), pp. 161-185.

De Goede, Marieke and Sullivan, Gavin (2015) 'The Politics of Security Lists', *Society and Space*, 0(0), pp. 1-22.

De Hert, Paul, Gutwirth, Serge, and Leenes, Ronald (2016) *Data Protection on the Move: Current Developments in ICT and Privacy-Data Protection*, Dordrecht, Netherlands: Springer.

Deibert, Ronald and Rohozinski, Rafal (2010) 'Risking Security: Policies and Paradoxes of Cyberspace Security', *International Political Sociology*, 4(1), pp. 15-32.

DeNardis, Laura (2014) *The Global War for Internet Governance*, New Haven, USA: Yale University Press.

Den Boer, Monica (2015) 'Counterterrorism, Security, and Intelligence in the EU: Governance Challenges for Collection, Exchange, and Analysis, *Intelligence and National Security*, 30(2-3), pp. 402-419.

Determann, Lothar (2016) 'Adequacy of Data Protection in the USA: Myths and Facts', *International Data Privacy Law*, 6(3), pp. 244-250.

Epstein, Richard (2016) 'The ECJ's Fatal Imbalance: Its Cavalier Treatment of National Security Issues Poses Serious Risk to Public Safety and Sound Commercial Practices', *European Constitutional Law Review*, 12(2), pp. 330-340.

Etzioni, Amitai (2015) 'NSA: National Security vs. Individual Rights', *Intelligence and National Security*, 30(1), pp. 100-136.

European Commission (2016) *Commission Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU - US Privacy Shield*, 12 July 2016, Available at: http://ec.europa.eu/justice/data- protection/files/privacy-shield-adequacy-decision en.pdf (Accessed 11 March 2017).

European Commission (2000) *Commission Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce*, 26 July 2000, Available at: http://eurlex.europa.eu/eli/dec/ 2000/520/oj (Accessed 15 March 2016).

European Parliament (2000) *Charter of Fundamental Rights Of The European Union*, 18 December 2000, Available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf (Accessed 13 March 2016).

European Parliament (1995) *Directive 95/46/EC of the European Parliament and of the Council*, 24 October 1995, Available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046 (Accessed 14 March 2016).

European Parliament (2006) *Directive 2006/24/EC of the European Parliament and of the Council*, 15 March 2006, Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2006.105.01.0054.01.ENG (Accessed 14 March 2016).

European Parliament (2016) *Regulation 2016/679 of the European Parliament and of the Council*, 4 May 2016, Available at: http://eur-lex.europa.eu/legal-content/EN/ TXT/PDF/?uri=CELEX:32016R0679&from=EN (Accessed 9 January 2017).

Fabbrini, Federico (2015) 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States', *Harvard Human Rights Journal*, 28(1), pp. 65-95.

Farrell, Henry and Newman, Abraham (2016) 'The Transatlantic Data War: Europe Fights Back Against the NSA', *Foreign Affairs*, January/February 2016, pp. 124-133.

Fitzgerald, Gary (2016) 'Schrems II-An Unnecessary Legal Frolic?' *Data Protection Ireland*, 9(4), pp. 9-11.

Fundamental Rights Agency of the European Union (2014) *Handbook on European Data Protection Law*, Brussels, Belgium: Council of Europe.

Galič, Maša, Koops, Bert-Jaap, and Timan, Tjerk (2016) 'Bentham, Deleuze, and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation', *Philosophy and Technology*, May 2016, pp. 1-29.

Gitelman, Lisa (2013) *Raw Data is an Oxymoron*, Cambridge, USA: MIT Press.

Gralla, Preston (2007) How the Internet Works, 8th edition, Indianapolis, USA: Que Publishing.
Hansen, Lene and Nissenbaum, Helen (2009) 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53(4), pp. 1155-1175.

Hassard, John and Law, John (1999) *Actor-Network Theory and After*, Oxford, UK: Blackwell Publishing.

Helgesson, Karin Svedberg and Mörth, Ulrika (2012) *Securitization, Accountability, and Risk Management: Transforming the Public Security Domain*, Abingdon, UK: Routledge.

Huysmans, Jef (2016) 'Democratic Curiosity in Times of Surveillance', *European Journal of International Security*, 1(1), pp. 73-93.

Huysmans, Jef (2014) *Security Unbound: Enacting Democratic Limits*, Abingdon, UK: Routledge.

Huysmans, Jef (2011) 'What's In An Act? On Security Speech Acts and Little Security Nothings', *Security Dialogue*, 42(4-5), pp. 371-383.

Jaatinen, Tanja (2016) 'The Relationship Between Open Data Initiatives, Privacy, and Government Transparency: A Love Triangle', *International Data Privacy Law*, 6(1), pp. 28-38.

Kaunert, Christian and Léonard, Sarah (2013) *European Security, Terrorism, and Intelligence: Tackling New Security Challenges in Europe*, Basingstoke, UK: Palgrave Macmillan.

Kennedy, Helen, Poell, Thomas, and Van Dijck, Jose (2015) 'Data and Agency', *Big Data and Society*, 2(1), pp. 1-7.

Kitchin, Rob (2014a) 'Big Data, New Epistemologies, and Paradigm Shifts', *Big Data and Society*, 1(2), pp. 1-12.

Kitchin, Rob (2014b) *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*, London, UK: SAGE Publications.

Kobrin, Stephen J. (2004) 'Safe Harbors Are Hard to Find: The Transatlantic Data Privacy Dispute, Territorial Jurisdiction, and Global Governance', *Review of International Studies*, 30(1), pp. 111-131.

Kong, Lingjie (2010) 'Data Protection and Transborder Data Flow in the European and Global Context', *The European Journal of International Law*, 21(2), pp. 441-456.

Koops, Bert-Jaap (2011) 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the Right to Be Forgotten in Big Data Practice', *SCRIPTed*, 8(3), pp. 1-28.

Koops, Bert-Jaaps (2014) 'The Trouble with European Data Protection Law', *International Data Privacy Law*, 4(4), pp. 250-261.

Krause, Keith and Williams, Michael C. (1996) 'Broadening the Agenda of Security Studies: Politics and Methods', *Mershon International Studies Review*, 40(2), pp. 229-254.

Kremer, Jan-Frederik and Müller, Benedikt (2014) *Cyberspace and International Relations: Theory, Prospects, and Challenges*, London, UK: Springer.

Kuner, Christopher (2015a) 'Data Nationalism and its Discontents', *Emory Law Journal*, 64(0), 2089-2098.

Kuner, Christopher (2015b) 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law, *International Data Privacy Law*, 5(4), pp. 235-245.

Kuner, Christopher (2009) 'Onward Transfers of Personal Data Under the US Safe Harbor Framework', *Bureau of National Affairs Privacy and Security Law Report*, August 2009, pp. 1-6.

Kuner, Christopher (2011) 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future', *OECD Digital Economy Papers*, No. 187, pp. 1- 39.

Kuner, Christopher (2013b) *Transborder Data Flows and Data Privacy Law*, Oxford, UK: Oxford University Press.

Langford, Duncan (2000) *Internet Ethics*, Basingstoke, UK: Macmillan Press.

Latour, Bruno (2011) 'Networks, Societies, Spheres: Reflections of an Actor-Network Theorist', *International Journal of Communication*, 5(0), pp. 796-810.

Latour, Bruno (2005) *Reassembling the Social: An Introduction to Actor-Network Theory*, New York, USA: Oxford University Press.

Laudati, Laraine (2015) *EU Court Decisions Relating to Data Protection*, Brussels, Belgium: European Anti-Fraud Office.

Law, John and Singleton, Vicky (2014) 'ANT, Multiplicity, and Policy', *Critical Policy Studies*, 8(4), pp. 379-396.

Lupton, Deborah (2015) *Digital Sociology*, Abingdon, UK: Routledge.

Lupton, Deborah and Michael, Mike (2015) 'Toward a Manifesto for the Public Understanding of Big Data', *Public Understanding of Science*, 25(0), pp. 1-13.

Lyon, David (2002) 'Everyday Surveillance: Personal Data and Social Classifications', *Information, Communication & Society*, 5(2), pp. 242-257.

Lyon, David (2014) 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique', *Big Data & Society*, 1(2), pp. 1-13.

Lyon, David (2006) *Theorizing Surveillance: The Panopticon and Beyond*, Portland, UK: Routledge.

McDonald, Matt (2008) 'Securitization and the Construction of Security', *European Journal of International Relations*, 14(4), pp. 563-587.

McDermott, Yvonne (2017) 'Conceptualizing the Right to Data Protection in an Era of Big Data', *Big Data and Society*, 4(1), pp. 1-7.

Michael, Mike (2017) *Actor-Network Theory: Trials, Trails, and Translations*, London, UK: Sage Publications Ltd.

Moulds, Richard (2014) 'The Global Data Protection Conundrum', *Network Security*, January 2014, pp. 16-17.

Müller, Martin (2015) 'Assemblages and Actor-Networks: Rethinking Socio-material Power, Politics, and Space', *Geography Compass*, 9(1), pp. 27-41.

Nexon, Daniel and Pouliot, Vincent (2013) 'Things of Networks: Situating ANT in International Relations', *International Political Sociology*, 7(3), pp. 342-345.

Ni Loidean, Nora (2016) 'The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law', *Journal of Internet Law*, 19(8), pp. 7-14.

Peoples, Columba and Vaughan-Williams, Nick (2015) *Critical Security Studies: An Introduction,* 2nd edition, New York, USA: Routledge.

Poulin, Chris (2014) 'Big Data Custodianship in a Global Society', *SAIS Review*, 34(1), pp. 109- 116.

Regan, Priscilla M. (2003) 'Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows', *Journal of Social Issues*, 59(2), pp. 263-282.

Rubinstein, Ira S. (2013) 'Big Data: The End of Privacy or a New Beginning?' *International Data Privacy Law*, 3(2), pp. 74-87.

Salter, Mark B. (2015) *Making Things International 1: Circuits and Motion* Minneapolis, USA: University of Minnesota Press.

Shimanek, Anna E. (2001) 'Do You Want Milk With Those Cookies? Complying With The Safe Harbor Privacy Principles', *Journal of Corporation Law*, Winter 2001, pp. 455-477.

Strauss, Stefan (2015) 'Datafication and the Seductive Power of Uncertainty- A Critical Exploration of Big Data Enthusiasm', *Information*, 6(4), pp. 836-847.

Svantesson, Dan Jerker B. (2013) 'A Layered Approach to the Extraterritoriality of Data Privacy Laws', *International Data Privacy Law*, 3(4), pp. 278-286.

Tene, Omer (2011) 'Privacy: The New Generations', *International Data Privacy Law*, 1(1), pp. 15-27.

Tracol, Xavier (2016) 'Invalidator Strikes Back: The Harbor Has Never Been Safe', *Computer Law & Security Review*, 32(2), pp. 345-362.

Turner, Brian S. (2009) *The Blackwell Companion to Social Theory*, Chichester, UK: Blackwell Publishing Ltd.

Van der Sloot, Bart (2014) 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation', *International Data Privacy Law*, 4(4), pp. 307-325.

Walker, Russell (2015) *From Big Data to Big Profits: Success with Data and Analytics*, Oxford, UK: Oxford University Press.

Weber, Rolf W. (2013) 'Transborder Data Transfers: Concepts, Regulatory Approaches, and New Legislative Initiatives', *International Data Privacy Law*, 3(2), pp. 117-130.