David Haynes – Edinburgh Napier University, United Kingdom

Understanding Personal Online Risk to Individuals via Ontology Development

Abstract

The concept of risk is widely misunderstood because of the different contexts in which it is used. This paper describes the development of an ontology of risk as a way of better understanding the nature of the potential harms individuals are exposed to when they disclose personal data online. The ontology was designed to be compatible with BFO, the Basic Formal Ontology (Arp, Smith, and Spear 2015). BFO is a top-level ontology which is intended to promote interoperability. Ontologies from domains such as genetics and medical research are in many instances designed to conform to BFO. An initial exercise to monitor the online activity of six participants from the library and information services community helped to identify the points at which personal data is disclosed during online activity. It also explored the motivations for these disclosures, by questioning participants about their perceptions of risk. The resulting analysis suggested that an ontology would be better than a typology to represent the complex relationships between risk concepts. Rosenblum (2007) developed a typology of risks associated with online social networking services (SNSs). Haynes and Robinson (2015) looked at personal risk derived from generic risk categories (Swedlow et al. 2009, 237). Terms were also extracted from existing terminologies (Sophos Ltd 2014; NIST 2019; Daniel J. Solove 2006). Risk scenarios were developed and tested during a formative seminar and incorporated into the ontology. Potential applications of the ontology include its use as a tool for interrogating large data sets about online activity, to identify when individuals may be exposed to privacy risk. This could be used to identify clusters of risk and map the factors that contribute to specific risks.

1. Introduction

1.1 Background

This research arose from an investigation into the nature of the risks associated with online disclosure of personal information. Interactions with online systems and social media platforms use an economic model based on the sale of personal data (Enders et al. 2008). Digital advertising income relies on monitoring online behaviour to build up profiles of individuals' interests. These profiles (whether anonymised or not) can then be used to match advertising to individuals. Different platforms gather quite different levels of data. This has been a remarkably effective model that has led to the growth of the largest companies in the world, so that for instance Facebook was able to announce profits of $18.5 billion on revenue of $70.7 billion in 2019 (Facebook 2020).

In return for disclosing personal data and allowing corporations to use that data, individuals gain 'free' access to services and online resources. Evidence suggests that when faced with risk or uncertainty, feelings (or affect) should be considered alongside rational (or cognitive-consequentialist) decision making (Loewenstein et al. 2001; Finucane and Holup 2006). Behaviour models tend to emphasise conscious, rational decision-making during online transactions involving personal data (Kehr et al. 2015). When an individual selects the 'allow cookies' option, they are facilitating access to their personal data in exchange for access to services. This has been characterised by many researchers as the 'privacy calculus'. The fact that individuals use these services suggests that the perceived benefits are judged to outweigh the perceived risks of disclosure.

1.2 Why it is topical

Individual risk and public safety are a focus for current UK government policy (DCMS 2019). In the European Union privacy concerns have been reflected in the General Data Protection Regulation (GDPR), which came into force in 2018 (European Parliament 2016). The principles-based approach adopted by EU countries and their partners has continued to evolve and is in contrast with the sectoral approach adopted in the United States (D J Solove and Hoofnagle 2006).

The purpose of this research is to understand the nature of the risks faced by individuals when they conduct online transactions. The description and categorizing of risks may help with the delivery of more effective mechanisms for managing those risks.

It could be argued that the purpose of regulation is to manage risk (Baldwin, Cave, and Lodge 2010). Although legislation is primary means of regulation adopted by government, it is not the full picture. Lessig (2006) encapsulated one aspect of internet regulation by the phrase "Code is Law". The way in which systems are designed affects the way in which they operate and is also a form of regulation. Cavoukian (2012) extended this idea with the concept of 'privacy by design'. Previous research suggests that a number of regulatory mechanisms (coding, self-regulation, market response and law) work in concert to regulate access to personal data on social networks (Haynes, Bawden, and Robinson 2016). Mapping the risks and their relationship with causes and effects may produce better insights into effective responses to this public safety issue.

1.3 Research question

This research sets out to examine the nature of the risks faced by individuals when they engage in online activity. The research considers the following questions:

- What is the nature of the risks that individuals face when using the internet?
- Is there an existing typology of online risk?
- Can an ontology of risk be developed to represent risk relationships more effectively than previous typologies of risk?

2. Literature review

2.1 Nature of online risk

Risk is an elusive concept, the definition of which depends on the context (Fischhoff, Watson, and Hope 1984). Aven and Renn (2009, 2) define risk in the following terms:

> "A. Risk is expressed by means of probabilities and expected values
> B. Risk is expressed through events/consequences and uncertainties"

Simply put, risk is the "effect of uncertainty on objectives" (ISO 2009, 1).

Aven et al (2011, 1079) make a distinction between risk as a concept and the way in which it is described or measured:

> "Risk should also exist as a concept without modeling or any other tool. We face risk when we drive a car or run a business even if the probabilities are not specified. For risk assessment we need the probabilities, but not as a general concept of risk. In this way we obtain a sharp distinction between risk as a concept (a), and risk descriptions (assessments) (c) which could be based on models (b)."

Impact and probability are two measures widely associated with risk management, the objective normally being to reduce or eliminate one or both of these measures.

A risk is based on an uncertain event (i.e. it has a probability of <1.0 of occurring). The risk event, or incident will have a measurable impact on the outcomes of the system that it is being considered in.
Risk applies to individuals, organizations, governments and societies. Cybersecurity has been a particular concern of companies for some time (Tuttle 2013; Prislan 2014; Biener, Eling, and Wirfs 2015). More recently there has been a concern about societal risk and public safety (DCMS 2019). When considering the risk to individuals it is necessary to make a distinction between risks to personal privacy and risks associated with disclosing personal data (e.g. via data breaches, as well as voluntary disclosure). The privacy calculus captures the concept of perceived individual risk as well as benefits associated with disclosure of personal data (Dinev and Hart 2006). Studies have found that there is an inverse correlation between severity of perceived risks and willingness to disclose personal data (Dinev and Hart 2006; Li, Sarathy, and Xu 2010).
Some studies have described the apparently paradoxical result where individuals disclose personal data despite perceived dangers associated with doing so (Gimpel, Kleindienst, and Waldmann 2018). Some of this can be put down to limitations in data gathering. Privacy paradox studies tend to depend on interviews with individuals about what they would do in hypothetical situations (Gimpel, Kleindienst, and Waldmann 2018; Min and Kim 2015; Bandara, Fernando, and Akter 2017). Work by Acquisti (2005) suggested that there is a discrepancy between intention and actual behaviour.

2.2 Using an ontology to describe risk

This research initially set out to develop a taxonomy of risk based on harm to individuals. This would allow hierarchical relationships between concepts. Entities in a taxonomy can be grouped by common origin (phylogeny) or by similarity (morphology) (Gnoli 2017) and this represents one way forward.
Solove (2006) provides a classification of harms, which is a starting point for categorizing risks. These largely predate the advent of social media and are in need of update to incorporate the spectrum of online harassment which can range from bullying through to hate speech. Issues such as disclosure and exposure have evolved into specific activities such as doxing. In these instances the focus is on the incident rather than the consequences to the individual.
Skinner et al (Skinner, Song, and Chang 2006) developed a taxonomy of risk based on three dimensions or views: time, space and matter. This was specifically developed in the context of collaborative environments and needs validation with empirical data.
Wright and Raab (2014, 290–91) identify examples of harms based on privacy principles. These both feed into an initial identification of online harms. Haynes and Robinson (2015) set these risks in a network of interconnected risks and consequences.

2.3 Complexity of relationships and ontologies

Standards for describing relationships between concepts have evolved from simple hierarchies displayed in classification schemes to the broader, narrower and related terms in thesauri (ISO 2011). The decision to use an ontology was based on the ability to define classes of concept and to describe different types of relationship between those classes.

Ontology development has been extensive in the biomedical area and this provides a corpus of experience that can be applied elsewhere. Some attention has been paid to other domains such as project management, business processes and cyber security, either using ontologies as a tool for risk assessment (McKone and Feng 2015; Scheuer, Haase, and Meyer 2013; Mohammad et al. 2015) or as a means of mapping the relationships between different elements of risk and specific instances of risk events. Perhaps the most directly relevant work is the review of ontologies covering cyber risk which seemed to emphasise vulnerabilities and exploitation by an attacker. There was less emphasis on the concepts of likelihood and impact, which were included in only 3 of the 10 ontologies reviewed by Oltramari and Kott (2018). The authors highlight the problem of estimating probabilities and impact levels in a dynamic environment where the behaviour of a target affects the outcomes. So, for instance if a targeted organization improves its security measures, a potential attacker will switch their attention to another, more vulnerable target. They also speculate that it is impossible to determine the outcomes without knowing more about the motivation of the attackers.

Zaitsev and Bunker (2016) developed an ontology of outsourcing risks which concentrates on the nature of the relationships between different risks. Risks are not analysed into likelihood and impact because the authors consider them to be dependent on context. By describing the strength of the relationship between risk, the ontology is intended as a "risk taxonomy tool that could be used for assessment of project risks." (Zaitsev and Bunker 2016, 11)

An ontology of online risk needs to reflect the complex nature of risk and the need to incorporate classes of concept such as: Vulnerability, Threat, Incident, Consequence, Harm and Response. Some of these classes also have properties that are defined in their schemas. For example, it might be useful to incorporate the idea of impact of a Harm or the Probability of an Event into the description of a risk scenario.

3. Methods

3.1 Creation of the ontology

Early prototyping used the Graphite system provided via the Synaptica interface. This was intuitive and allowed experimentation with different data formats and development of schemas. This development environment allows export into an OWL-compatible system so that it can plug into high-level ontologies such as the Basic Formal Ontology (BFO).

There are many approaches to the development of a knowledge organization system and in particular the development of an ontology. The ideas put forward by Arp et al (2015) have been widely adopted and provided the basis for the development of the ontology for this project. The authors talk about four general principles of ontology design:

1. Realism – an ontology is a representation of reality, which is supported by evidence and observation
2. Perspectivalism – reality is too complex to be represented by a single approach. Ontologies should therefore aim to be relevant and accurate within a specified domain

3. Fallibilism – an ontology will change as our understanding and knowledge of a domain develops. It is therefore necessary to be able to keep track of different versions of an ontology and the changes made
4. Adequatism – room must be made for all the types of entity that exist within the domain of the ontology

Plus some additional principles:

5. The principle of reuse
6. Balance between utility and realism
7. Open-ended design process
8. Low-hanging fruit

Arp et al (2015, 44) suggest that ontologies are representations of reality rather than models of reality based on mental concepts:

> "Realism in ontology is based further on the idea that with the aid of science we can come to know the general features of reality in the form of universals and the relations between them. This realist approach has a number of general consequences. First, it implies that ontologies are representations of reality, not of people's concepts or mental representations or uses of language."

This presents some real challenges in dealing with human behaviour and motivations. When looking at privacy this research is concerned with motivations to disclose personal data online and the harms (and benefits) that might result. The harms themselves may depend on the perceptions of the individual, so that similar events might be viewed very differently by different individuals.

What is the 'reality' we are trying to represent with this ontology? The fact of people's perceptions is a reality that is captured in attitudinal surveys. They provide a snapshot if what people thought at a particular point in time – and of course they may change in light of experience, a better understanding of online harms or education about privacy risks. It is possible to 'de-construct' an event such as a data breach or a phishing attack into elements of risk.

Risk can be seen as part of the ontology of social reality rather than objective reality, because it depends on agency: "risk belongs to this subjective ontology [of social reality]. Thus, risks are real, but only insofar as there is a social reality in which subjects engage in risk taking." (Merkelsen 2011, 894).

The ontology is built up using concept s that are defined in the following terms: "The recommended best practice for creating definitions along the lines described earlier is to use the Aristotelian form: S = def. a G that Ds" (Arp, Smith, and Spear 2015, 69).

3.2 Choice of software

The ontology was designed to be hospitable to RDF data to allow for import from other ontologies and export of the resulting ontology to new environments. The Protégé system developed at Stanford was considered as a suitable platform because it is widely used and has an active community of developers. It supports OWL, which is a W3C standard. The Synaptica Graphite system was also considered for this exercise and was eventually selected because of the support available to the researcher. It is a commercial product that was made available at no charge for the purposes of this research. It has inbuilt visualisation tools and allows export of RDF data from the ontology.

3.3 Development of the ontology

The methodology for development of the ontology was described in a previous paper (Haynes 2019). Noy and McGuiness' (2001) iterative approach was adopted and applied to the seven-step method for ontology development of Arp et al (2015):

1. Determine scope
2. Reuse existing ontologies
3. Enumerate important terms
4. Define classes and class hierarchy
5. Define class properties
6. Define facets of the slots
7. Create instances

3.4 Testing and validation

The ontology design was tested in a seminar with 14 researchers and practitioners with backgrounds in: knowledge organization, information governance, cybersecurity and information science. Participants worked in groups to examine the proposed representation of risk and to provide a critique to refine it.

An initial set of risk incidents was incorporated into the ontology as a set of scenarios, based on standard definitions and on descriptions in the literature. A degree of normalisation was required for consistency.

Seminar participants were asked to explore risk scenarios to identify the consequents and harms that could result from an incident. They were also asked to consider the causes that contributed to the incident. The responses were consolidated and expressed as relationships, which entered into the ontology.

The relationship network was then explored and graphs generated to illustrate the connection between different entities in the ontology.

3.5 Visualization of graphs

The graphs representing the relationships were shown using the visualization tool within the Synaptica Graphite system. This is an interactive system that allows exploration of the relationship between nodes and navigation through the landscape of risks, their causes and consequences.

Exporting the ontology to a data visualization environment allows the possibility of using visualization for debugging the ontology (Chapman and Roberts 2018). This will be considered for future development and for possible integration with a high-level ontology such as BFO.

4. Results

4.1 Scope of the ontology

The scope of the ontology was defined during the early stage of the project and was based on the overall objective of better understanding risk to individuals. The scope of the onotology is described more fully in Haynes (2019, 171–72) and can be summarised as follows:

The ontology covers online hazards faced by online users and the resulting consequences and harms to the individual. It shows the cause and effect relationships between threats, incidents and consequences of disclosing personal data online. The main purpose of the ontology is to map different types of hazards that individuals face and the possible mitigating actions that they could take. It will also identify similarities between different hazards and to identify ways in which they might be addressed.

4.2 Evolution of the representation of risk in the light of feedback

During the workshop, the initial representation was endorsed with some modifications to align it more closely with the cybersecurity view of risk rather than the project management view. Figure 1 shows the initial outline ontology.

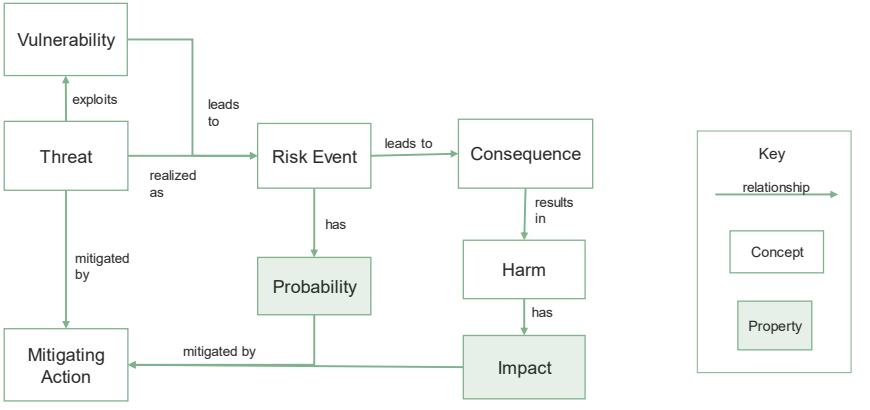

Figure 1- Initial Representation of Risk

Figure 2 shows the revised representation of risk, which incorporates feedback from the validating workshop. Risk is now defined in terms of threats that exploit vulnerabilities in systems. The threats could be malicious or accidental. Risk events are classed as Incidents. Instead of just mitigating actions to lessen the impact of an incident, there are also avoiding actions and defending actions to reduce the likelihood of an incident and to reduce or eliminate the threat and/or vulnerability of a system. There was some discussion about whether consequence and harm should be separated. Examination of instances of this representation suggest that it is useful to distinguish between the consequence of an incident and the harm to an individual. For example, during a data breach incident, personal bank account details might fall into the hands of criminals and the harm to the individual might be loss of money. The harm is not necessarily realised because the bank may for instance take mitigating action, or the criminals might fail to exploit the data.

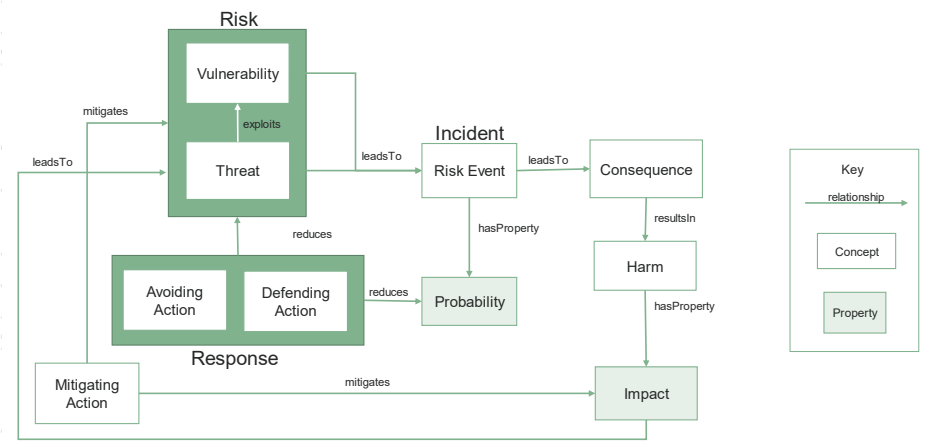

Figure 2- Modified Representation of Risk

4.3 Scenarios

A set of scenarios was developed from reports in the literature, the case studies conducted with the volunteers and development of scenarios during the workshop. Table 1 lists the scenarios used to test different types of risk faced by individuals. They were used to explore the relationships between the causes of a risk and its consequences and these were captured in the ontology.

Table 1 - Scenarios used to develop the ontology

Risk	Incident scenario
CLICK-BAIT	Fall down a click-bait rabbit hole
CLOUD STORAGE	Data breach of cloud documents
DIGITAL ASSISTANTS	Digital assistant self-launches
ILLEGAL SITE	Visit an illegal site
LOCATION TRACKING	Location tracking made public
NON-SECURE SITE	Land on non-https site
ONLINE BANKING	Bank login details revealed
ONLINE PURCHASES	Data breach of online purchase transaction
OUT-OF-DATE SOFTWARE	Use out of date software
PHISHING	Respond to phishing email
PICTURES ON SOCIAL MEDIA	Hostile response to photo posted on social media
PROFESSIONAL NETWORKS	Employer discovers job-seeking activity
RE-USE OF PASSWORDS	Re-used password is detected

4.4 Exploring the network of relationships

The modified representation of risk is based on different relationships between the concept classes. Table 2 shows the classes and their relationships within the ontology. Many of these relationships have reciprocals. So for instance, the top term ‘Psychological harm’ in the ontology scheme Harm, has narrower terms: ‘Annoyance’,

'Fear' and 'Worry'. Each of these has a reciprocal broader term relationship with 'Psychological harm'.

Table 2 - Relationships allowed between concepts in different classes

Subject (class)	Predicate	Object (class or property)
Consequence	broader	Consequence
Consequence	leadsTo	Consequence
Consequence	leadsTo	Harm
Consequence	narrower	Consequence
Harm	broader	Harm
Harm	hasProperty	Impact
Harm	narrower	Harm
Incident	broader	Incident
Incident	hasProperty	probability
Incident	LeadsTo	Incident
Incident	leadsTo	Consequence
Incident	leadsTo	Threat
Incident	narrower	Incident
Response	broader	Response
Response	mitigates	Impact
Response	mitigates	Incident
Response	mitigates	Harm
Response	mitigates	Consequence
Response	mitigates	Threat
Response	mitigates	Vulnerability
Response	narrower	Response
Threat	exploits	Vulnerability
Threat	leadsTo	Incident
Vulnerability	broader	Vulnerability
Vulnerability	leadsTo	Incident
Vulnerability	narrower	Vulnerability

Figure 3 shows an example of an incident and its relationship to other concepts in the ontology. A 'breach of cloud storage' is a scenario in the Incident scheme. It is a consequence of 'use of cloud services' (a prerequisite in event tree analysis) and/or 'data theft'. It leads to 'loss of confidentiality' and 'consequential loss'. The figure

also shows the relationship to Schemas, Resource types, Templates and Collections.

Figure 3- Example of a concept and its relationships

Navigating to the concepts that led to the incident reveals their network of relationships as seen in Figure 4. From this we learn that Use of Cloud Services is a vulnerability and that has a number of subordinate relationships (for the sake of simplicity we have used broader and narrower term relationships here). Data theft on the other hand is classed as a threat because it implies intent on the part of an agent. Other threats might result from a natural phenomenon such as a solar storm or lightning strike that could lead to data loss.

Figure 4 - Conditions that could lead to a breach of cloud storage

Figure 5 shows that a breach of cloud storage could lead to loss of confidentiality, which in turn could lead to loss of reputation (a harm). Loss of confidentiality could also result from the self-launch of a digital assistant. There are likely to be other incidents that could lead to this consequence, demonstrating much greater complexity than a simple hierarchical classification could handle. The breach could also lead to a consequential loss resulting in financial loss to an individual, another harm. Some relationships are two way. For instance, 'Breach of cloud storage' could be both a cause and a consequence of 'Loss of confidentiality'.

Figure 5 - Consequences of a breach of cloud storage

4.5 Inferences from the ontology

As well as providing a helpful visual display of the relationships between different aspects of risk, the ontology allows navigation and exploration of different aspects of risk. This could be valuable in tracking relationships and identifying connections that are not immediately obvious on initial inspection. The next stage of the research will be to consider the eigenvector values of each node to determine closeness and identify potential clusters of concepts (Hansen, Schneiderman, and Smith 2011). This may reveal deeper structure in the set of scenarios in the ontology.

5. Discussion and conclusion

5.1 Addressing the research questions

The project set out to explore the nature of risks that individuals face when using the internet and to develop a risk taxonomy. Taxonomies are based on hierarchical relationships and do not allow for the complex relationships between risk concepts. For this reason, an ontology was developed instead. It was based on pre-existing work as well as industry definitions of vulnerability and threats (Haynes 2019). However, these definitions tended to be focused on technical issues and consequences to systems, or organizations. This ontology shifts the focus on to people and the impact of online incidents on individuals. It explores by means of scenarios the relationships between

Vulnerabilities, Threats and Incidents and then the outcomes of Incidents in terms of Consequences and Harms. The ontology also includes responses that could mitigate these risks.
Although several broad categorizations of risk were identified, they tended to be very broad and did not represent the complex web of relationships between causes (threat and vulnerability concepts) and effects (consequences and harms).

5.2 Limitations

The ontology could be developed further by continuing to add scenarios. The analysis of scenarios is based on one researcher's interpretation of data gathered from a small group of experts. To some extent this is subjective and needs a more rigorous evaluation – possibly by means of a Delphi study. This would allow a panel of experts to arrive at a consensus about the concepts and relationships associated with the scenarios.

5.3 Future Development

The next stage of development for this ontology is to populate it with instances from a variety of source, including reports in the press, incident data from data protection regulators and case studies in the literature. This would test how well the scenarios describe the reality of online risks to individuals. It would also provide the groundwork for creation of linked data sets, which could be analysed to inform policy on online safety.

Acknowledgement

This research was supported by the Royal Academy of Engineering and the Office of the Chief Science Adviser for National Security under the UK Intelligence Community Postdoctoral Fellowship Programme (Grant No. ICRF1718\1\54). The Graphite system used to develop the ontology was provided by Synaptica Ltd. The research was conducted during Dr Haynes' Fellowship at the Department of Library and Information Science at City, University of London. Thanks to the anonymous reviews for their valuable comments and suggestions. Finally, the author would like to acknowledge the advice of colleagues in the School of Computing at Edinburgh Napier University.

References

Acquisti, Alessandro, and Jens Grossklags. 2005. "Privacy and Rationality in Individual Decision Making." *IEEE Security & Privacy* 3 (1): 26–33.

Arp, R., B. Smith, and A.D. Spear. 2015. *Building Ontologies with Basic Formal Ontology*. Cambridge, MA: MIT Press eBooks Library.

Aven, T., O. Renn, and E.A. Rosa. 2011. "On the Ontological Status of the Concept of Risk." *Safety Science* 49 (8): 1074–79.

Aven, Terje, and Ortwin Renn. 2009. "On Risk Defined as an Event Where the Outcome Is Uncertain." *Journal of Risk Research* 12 (1): 1–11. https://doi.org/10.1080/13669870802488883.

Baldwin, Robert, Martin Cave, and Martin Lodge, eds. 2010. *The Oxford Handbook of Regulation*. Oxford Handbooks in Business and Management. Oxford: Oxford University Press.

Bandara, Ruwan, Mario Fernando, and Shahriar Akter. 2017. "The Privacy Paradox in the Data-Driven Marketplace: The Role of Knowledge Deficiency and Psychological Distance." *Procedia Computer Science* 121: 562–67. https://doi.org/10.1016/j.procs.2017.11.074.

Biener, Christian, Martin Eling, and Jan Wirfs. 2015. "Insurability of Cyber Risk: An Empirical Analysis[Dagger]." *Geneva Papers on Risk & Insurance* 40 (1): 131–58. https://doi.org/10.1057/gpp.2014.19.

Cavoukian, Ann. 2012. "Privacy by Design [Leading Edge]." *IEEE Technology and Society Magazine* 31 (4): 18–19.

Chapman, P, and W Roberts. 2018. "Towards Diagram-Based Editing of Ontologies." In *Diagrammatic Representation and Inference*, 699–703. https://doi.org/10.1007/978-3-319-91376-6_62.

DCMS. 2019. "Online Harms White Paper." London. https://doi.org/978-1-5286-1080-3.

Dinev, Tamara, and Paul Hart. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions." *Information Systems Research* 17 (1): 61–80. https://doi.org/10.2307/23015781.

Enders, Albrecht, Harald Hungenberg, Hans-Peter Denker, and Sebastian Mauch. 2008. "The Long Tail of Social Networking." *European Management Journal* 26 (3): 199–211. https://doi.org/10.1016/j.emj.2008.02.002.

European Parliament. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN.

Facebook. 2020. "Facebook Q4 2019 Results." 2020. https://s21.q4cdn.com/399680738/files/doc_financials/2019/q4/Q4-2019-Earnings-Presentation-_final.pdf.

Finucane, Melissa L, and Joan L Holup. 2006. "Risk as Value: Combining Affect and Analysis in Risk Judgments." *Journal of Risk Research* 9 (2): 141–64. https://doi.org/10.1080/13669870500166930.

Fischhoff, Baruch, Stephen R Watson, and Chris Hope. 1984. "Defining Risk." *Policy Sciences* 17 (2): 123–39.

Gimpel, Henner, Dominikus Kleindienst, and Daniela Waldmann. 2018. "The Disclosure of Private Data: Measuring the Privacy Paradox in Digital Services." *Electronic Markets* 28 (4): 475–90. https://doi.org/10.1007/s12525-018-0303-8.

Gnoli, Claudio. 2017. "Classifying Phenomena Part 2: Types and Levels." *Knowledge Organization* 44 (1): 37–54. https://doi.org/10.5771/0943-7444-2017-1-37.

Hansen, Derek L, Ben Schneiderman, and Marc A Smith. 2011. *Analyzing Social Media Networks with NodeXL: Insights from a Connected World*. Burlington, MA: Morgan Kaufmann Publishers.

Haynes, David. 2018. *Metadata for Information Management and Retrieval: Understanding Metadata and Its Use*. 2nd ed. London: Facet Publishing.

———. 2019. “Creating an Ontology of Risk: A Human-Mediated Process.” In The Human Position in an Artificial World: Creativity, Ethics and AI in Knowledge Organization. ISKO UK Sixth Biennial Conference London 15-16th July 2019, edited by David Haynes and Judi Vernau, 167–80. Baden-Baden: Ergon Verlag GmbH.

Haynes, David, David Bawden, and Lyn Robinson. 2016. “A Regulatory Model for Personal Data on Social Networking Services in the UK.” *International Journal of Information Management* 36 (6): 872–82. https://doi.org/10.1016/j.ijinfomgt.2016.05.012.

Haynes, David, and Lyn Robinson. 2015. “Defining User Risk in Social Networking Services.” *Aslib Journal of Information Management* 67 (1): 94–115.

ISO. 2009. “ISO 31000:2009 Risk Management — Principles and Guidelines.” Geneva.

———. 2011. “ISO 25964-1:2011 - Information and Documentation — Thesauri and Interoperability with Other Vocabularies. Part 1: Thesauri for Information Retrieval.” Geneva.

Kehr, Flavius, Tobias Kowatsch, Daniel Wentzel, and Elgar Fleisch. 2015. “Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus.” *Information Systems Journal* 25 (6): 607–35. https://doi.org/10.1111/isj.12062.

Lessig, Lawrence. 2006. *Code*. 2nd ed. New York; London: BasicBooks. http://codev2.cc/download+remix/Lessig-Codev2.pdf.

Li, Han, Rathindra Sarathy, and Heng Xu. 2010. “Understanding Situational Online Information Disclosure as a Privacy Calculus.” *Journal of Computer Information Systems* 51 (1): 62–71.

Loewenstein, George F, Elke U Weber, Christopher K Hsee, and Ned Welch. 2001. “Risk as Feelings.” *Psychological Bulletin* 127 (2): 267–86. https://doi.org/10.1037/0033-2909.127.2.267.

McKone, Thomas E, and Lydia Feng. 2015. “Building a Human Health Risk Assessment Ontology (RsO): A Proposed Framework.” *Risk Analysis* 35 (11): 2087–2101. https://doi.org/10.1111/risa.12414.

Merkelsen, Henrik. 2011. “The Constitutive Element of Probabilistic Agency in Risk: A Semantic Analysis of Risk, Danger, Chance, and Hazard.” *Journal of Risk Research* 14 (7): 881–97. https://doi.org/10.1080/13669877.2011.571781.

Min, Jinyoung, and Byoungsoo Kim. 2015. “How Are People Enticed to Disclose Personal Information Despite Privacy Concerns in Social Network Sites? The Calculus between Benefit and Cost.” *Journal of the Association for Information Science & Technology* 66 (4): 839–57.

Mohammad, Mahmud Abdulla, Ioannis Kaloskampis, Yulia Hicks, and Rossitza Setchi. 2015. “Ontology-Based Framework for Risk Assessment in Road Scenes Using Videos.” *Procedia Computer Science* 60 (C): 1532–41. https://doi.org/10.1016/j.procs.2015.08.300.

NIST. 2019. “National Vulnerability Database.” 2019. https://nvd.nist.gov/.

Noy, N. F., and D. L. McGuinness. 2001. “Ontology Development 101: A Guide to Creating Your First Ontology.” Stanford CA. https://protege.stanford.edu/publications/ontology_development/ontology101.pdf.

Oltramari, A, and A Kott. 2018. “Towards a Reconceptualisation of Cyber Risk: An Empirical and Ontological Study.” *Journal of Information Warfare* 17 (1): 49–73.

Prislan, Kaja. 2014. “Efficiency of Corporate Security Systems in Managing Information Threats: An Overview of the Current Situation.” *Varstvoslovje* 16 (2): 128–47.

Rosenblum, David. 2007. “What Anyone Can Know: The Privacy Risks of Social Networking Sites.” *IEEE Security & Privacy* 5 (3): 40–49.

Scheuer, Sebastian, Dagmar Haase, and Volker Meyer. 2013. “Towards a Flood Risk Assessment Ontology – Knowledge Integration into a Multi-Criteria Risk Assessment Approach.” *Computers, Environment and Urban Systems* 37: 82–94. https://doi.org/https://doi.org/10.1016/j.compenvurbsys.2012.07.007.

Skinner, G, H Song, and E Chang. 2006. “An Information Privacy Taxonomy for Collaborative Environments.” *Information Management & Computer Security* 14 (4): 382–92.

Solove, D J, and C J Hoofnagle. 2006. “A Model Regime of Privacy Protection.” *University of Illinois Law Review*, no. 2: 357–403.

Solove, Daniel J. 2006. “A Taxonomy of Privacy.” *University of Pennsylvania Law Review* 154 (3): 477–564. https://doi.org/10.2307/40041279.

Sophos Ltd. 2014. “Threatsaurus: The A-Z of Computer and Data Security Threat.” Oxford.

Swedlow, Brendon, Denise Kall, Zheng Zhou, James K Hammitt, and Jonathan B Wiener. 2009. “Theorizing and Generalizing about Risk Assessment and Regulation through Comparative Nested Analysis of Representative Cases.” *Law & Policy* 31 (2): 236–69.

Tuttle, Hilary. 2013. “Taking Cybersecurity Seriously.” *Risk Management* 60 (8): 18–19.

Wright, David, and Charles Raab. 2014. “Privacy Principles, Risks and Harms.” *International Review of Law, Computers & Technology* 28 (3): 277–98.

Zaitsev, Anna, and Deborah Bunker. 2016. “Developing an Ontological View of Outsourcing Risk, Risk Categories and Their Relationships Using Protege and OWL.” In *PACIS 2016*.