Risk, Hazards & Crisis in Public Policy
www.psocommons.org/rhcpp/

Risk, Hazards & Crisis in Public Policy, Vol. 00, No. 00, 2020

Risk Personalization: Governing Uncertain Collective Risk Through Individual Decisions

Shannon Spruit*, Mark de Bruijne and Wolter Pieters

Individuals are regularly made responsible for risks they wish to take: one can consent to processing of personal data, and decide what to buy based on risk information on product labels. However, both large-scale processing of personal data and aggregated product choices may carry collective risks for society. In such situations, governance arrangements implying individual responsibility are at odds with uncertain collective risks from new technologies. We, therefore, investigate the governance challenges of what we call risk personalization: a form of governance for dealing with uncertain collective risks that allocates responsibility for governing those risks to individuals.

We situate risk personalization at the intersection of two trends: governance of uncertain risk, and emphasis on individual responsibility. We then analyze three cases selected based on diversity: social media, nano-materials, and Uber. Cross-case comparison highlights issues of risk personalization pertaining to (i) the nature of the risk, (ii) governance arrangements in place, and (iii) mechanisms for allocating responsibility to individuals. We identify governance challenges in terms of (i) meaningful choice, (ii) effectiveness in mitigating risk, and (iii) collective decision making capacity. We conclude that the risk personalization lens stimulates reflection on the effectiveness and legitimacy of risk governance in light of individual agency.

KEY WORDS: collective risk, governance, innovation, risk, responsibilization, technology development

摘要

个人经常成为其希望承担的风险的负责人: 一个人能同意其个人数据被用于处理, 并基于产品标签上的风险信息决定购买哪些产品。然而, 个人数据的大型处理以及总产品选择可能为社会带来集体风险。在这样的情况下, 暗示个人责任的政府安排与源自新科技的不确定集体风险存在对立。因此, 我们研究了被称为"风险个人化"*(risk personalization)*的治理挑战:这是一种用于应对不确定集体风险的治理形式, 它将治理这些风险的责任分配给个人。

我们将风险个人化置于两个趋势的交汇处: 不确定风险治理、对个人责任的强调。我们随后基于社交媒体、纳米材料和*Uber*, 分析了三个案例。跨案例比较强调了以下与风险个人化相关的问题, *1)* 风险性质, *2)* 当前的治理安排, *3)*个人责任分配机制。我们识别了*3*个治理挑战, *1)* 有意义的选择, *2)* 在缓解风险方面的有效性, *3)* 集体决策能力。我们的结论认为, 风险个人化视角激发了与"就个人能力而言风险治理的有效性和合法性" 相关的反思。

关键词: 风险, 集体风险, 治理, 责任化, 创新, 技术开发

*Corresponding author: Shannon Spruit, P.O.Box 5015, 2600GA Delft, The Netherlands (S.L.Spruit@tudelft.nl)
Additional author affiliation information can be found at the end of this article.

doi: 10.1002/rhc3.12208

© 2020 The Authors. Risk, Hazards & Crisis in Public Policy published by Wiley Periodicals LLC on behalf of Policy Studies Organization
This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

Resumen

Las personas son regularmente responsables de los riesgos que desean asumir: se puede dar su consentimiento para el procesamiento de datos personales y decidir qué comprar en función de la información de riesgo en las etiquetas de los productos. Sin embargo, tanto el procesamiento a gran escala de datos personales como las opciones de productos agregados pueden conllevar riesgos colectivos para la sociedad. En tales situaciones, los arreglos de gobernanza que implican responsabilidad individual están en desacuerdo con los riesgos colectivos inciertos de las nuevas tecnologías. Por lo tanto, investigamos los desafíos de gobernanza de lo que llamamos personalización de riesgos: una forma de gobernanza para hacer frente a riesgos colectivos inciertos que asigna la responsabilidad de gobernar esos riesgos a las personas.

Situamos la personalización del riesgo en la intersección de dos tendencias: la gobernanza del riesgo incierto y el énfasis en la responsabilidad individual. Luego analizamos tres casos seleccionados en función de la diversidad: redes sociales, nanomateriales y Uber. La comparación de casos cruzados destaca los problemas de personalización del riesgo relacionados con 1) la naturaleza del riesgo, 2) los acuerdos de gobernanza establecidos y 3) los mecanismos para asignar responsabilidades a las personas. Identificamos los desafíos de gobernanza en términos de 1) elección significativa, 2) efectividad en la mitigación del riesgo y 3) capacidad de toma de decisiones colectivas. Concluimos que la lente de personalización del riesgo estimula la reflexión sobre la efectividad y legitimidad de la gobernanza del riesgo a la luz de la agencia individual.

PALABRAS CLAVES: riesgo, riesgo colectivo, gobernancia, responsabilización, innovación, desarrollo tecnológico

Introduction

As an individual, one can decide whether to give consent for processing personal data when downloading an app or visiting a website. This decision may reflect a trade-off between the benefits of using the service and the risks associated with misuse of the personal data involved. Similarly, one may assess the information on product labels in the decision what product to buy, for example in the case of cosmetics containing nanomaterials. Again, in making a choice one may weigh the positive effects of the product against the health risks of nanomaterials. However, collective risks such as large-scale processing of personal data by app providers and associated profiling and discrimination, or potential harmful effects of nanomaterials from large-scale use of cosmetics on the environment, may not be taken into account in such individual decisions. Furthermore, in both cases, it may not be clear whether enough information is available to make a well-founded decision.

Problem Statement

In this paper, we investigate the phenomenon that we call "risk personalization": a form of governance for dealing with uncertain collective risks that allocates responsibility for governing those risks to individuals. Where the effects of risk-taking are felt

by individuals themselves, such individualized risk governance arrangements may make a lot of sense. But the existence of tensions between collective risk and individual decisions is well-known, and for example described as a governance challenge in the tragedy of the commons (Hardin, 1968) and particularly in terms of technology development and modernization by Beck and Giddens (cf. Ekberg, 2007; Giddens, 1999).

We see governance arrangements involving individualized responsibility for risk emerging in many more cases in the context of new technology development, such as social media, nanotechnology, and taxi apps, where collective risks are a major issue, without appropriate discussion on these matters. Contrary to responsibilization, in which more individual responsibility is the *purpose* of or at least an explicit choice in governance, many developments have individual responsibility as a *consequence*, without explicit analysis or consideration of the pros and cons of this in terms of risk governance of collective risks. It is this class of issues that is the topic of this paper.

Our starting point is that applying or allowing for the development of personalized governance arrangements for uncertain *collective risks* may itself be risky in terms of recreating tensions between individual decisions and collective consequences. By analyzing these tensions in more detail for a diverse set of individual risk governance arrangements, associated governance challenges can be more specifically identified. This paper asks the question:

> *What are properties of and differences between governance arrangements in which responsibility for collective risks is allocated to individuals?*

Method

To understand the phenomenon better, two developments and their interactions in the governance of risk in today's risk society are described in more detail (i.e., governance of uncertain risk, and emphasis on individual responsibility) as an explanation of the constituents of the risk personalization concept.

Next, three empirical examples of risk personalization are explored; that is, cases where individuals bear responsibility for governing risks of new and uncertain technologies. Cases were selected based on diversity, that is, the diverse cases approach described by Seawright and Gerring (2008). The variables for which diversity is sought are (i) the nature of the risk and (ii) the existing governance arrangements in place. For the former, risk domains are selected which are strongly affected by new technology development (physical safety, data security, and environmental safety), focussing on both individual and collective components. For the latter, cases ranging from well-established and explicit arrangements for the individual governance of risk (strong governance) to more implicit forms of risk governance via risk personalization and an apparent lack of regulation (weak governance) were selected. Taking these considerations into account, privacy waivers on social media (data security, strong governance), the labeling of nanomaterial containing cosmetics (environmental safety, medium governance) and taxi

apps (Uber) and the responsibility for road safety (physical safety, weak governance) were selected.

The cases are explored and subsequently compared in a cross-case analysis to determine common properties and differences. The cross-case analysis is grounded in the framework provided by second section and identifies: (i) the risk domain and sources of uncertainty, (ii) the governance arrangement to deal with risks, and (iii) the way in which emphasis is put on individual responsibility. The relevant dimensions emerge from differences which could be observed in the different cases. The paper concludes by assessing and explaining how risk personalization helps as a lens for critically assessing current risk governance arrangements and the resulting challenges, extracting key challenges and policy implications of the governance scheme of risk personalization.

Theoretical Framework

In this section, the concept of risk personalization is developed, which is defined as a form of governance for dealing with uncertain collective risks that allocates responsibility for governing those risks to individuals. This is done by situating this concept against the background of the risk society, and highlighting major developments related to the governance of (collective) risks of new technologies: governance of uncertain risk and the fragmentation of governance regimes, and emphasis on responsibility of individuals.

Governance of Uncertain Risk

The understanding that new technologies can profoundly influence both the user of the technology as well as (unprepared) third parties is well known and addressed in fields such as public economics, sociology and law. Apart from generating potential risks for individual use, new technologies can produce collective risks, that is, their (negative) consequences can affect larger groups of people and the environment they live in (cf. Dorbeck-Jung & Bowman, 2017; examples are provided in Harremoës et al., 2001). Giddens (1999, p. 4) considers these examples of *manufactured risk*, that is, "risk created by the very progression of human development"; key indicators of the post-modernist "risk society," which creates as many new uncertainties and risks as those that are solved through scientific progress. A key challenge of the governance of new technologies has been how to deal with negative "externalities," which traditionally resulted in the development of institutions to govern collective risk (van Waarden, 2001). Examples of technologies that are primarily publicly governed via this regime are large-scale, complex and capital intensive technologies such as nuclear power, aviation, and more recently carbon capture and storage projects.

However, as predicted by Beck in the late 1980s, today's governance of new and uncertain technologies has become more decentralized and consequently also more fragmented as a result of a number of more generic centrifugal trends such as the increased role of markets and networks in governance (cf. Bevir, 2012) as well as the

rise of multi-level governance (i.e., the hollowing out of the state) and "the loss of functions upwards to the European Union, downwards to special-purpose bodies and outwards to agencies" (Rhodes, 1997, p. 17). Governments in western society have retreated in (risk) regulation from classes of (societal) risks, giving way to more complex, and diverse multi-level forms of governance in which different actors and stakeholders play a role (cf. Renn, Klinke, & Van Asselt, 2011).

Hood, Rothstein, and Baldwin (2001) identify "variations in the ways risks and hazards are handled across policy domains" (Hood et al., 2001, p. 6), resulting in an "archipelago" of risk domains in which modern states sometimes enforce risk regulation via heavy arrangements, whereas in other domains state governments have reduced their role and yielded to different risk regulatory regimes in which self-regulation or behavior of individuals or consumers plays a more important role (Hutter, 2010) introducing more distributed forms of responsibility for the governance of risk (Wiener, 2010, p. 140), making it both less obvious and more difficult to govern collective risks centrally, thereby providing fertile ground for risk personalization arrangements.

For example, with regard to natural hazards, citizens are "gradually transformed into risk managers and active participants of the multi-scale risk governance network as they are encouraged or even required to take more responsibility for their actions. This process of "responsibilization" (Garland, 1996) and "privatization of risk" (cf. Kuhlicke, 2011) pushes individuals to engage in risk governance.

In recent years, risk governance scholars and risk practitioners have reached similar conclusions as they found that classic risk management approaches do not suffice as governance regime for new technologies; other governance regimes are required under conditions of uncertainty (WRR, 2009). New technologies (especially the more disruptive ones) create new uncertainties about their impact (Beck, 1992). These may be hazards that turn out to be hard to quantify (known unknowns), but can also be undesirable consequences that were unconceivable at the time when the new technology entered the market (unknown unknowns) (Taleb, 2008). A well-known example of this last form of uncertainty can be found in CFCs as refrigerator coolants and their until the 70s largely unknown effects on the ozone layer (Mullin, 2002). It was precisely effects like this, that caused Beck to argue that "our collective safety, security, and survival are compromised because the anonymous and cumulative risks are characterized by organized irresponsibility, unaccountability and uninsurability" (Ekberg, 2007, p. 349).

To this end, state-of-the-art thinking in risk governance considers that the management of risk of new technologies needs to be thoroughly discussed between a wide range of stakeholder groups (Klinke & Renn, 2012; Renn & Schweizer, 2009). The basic tenet is that as expertise, agency and use of new technologies is distributed, so too should risk governance be. Instead of actively governing risk, governments have taken on a facilitating role, seeking to connect the various stakeholders to discuss risk.

Emphasis on Individual Responsibility

A key development resides in the changed role of individuals in decision making in general, and in responsibility for risk decisions in particular. In the

general sense, several analyses point to the fact that more choices can and should be made by individuals in contemporary society, increasing both the freedom and the responsibility of those individuals. This empirical and/or philosophical observation (or diagnosis) of modern society is what Beck (1992) refers to as individualization.

At the same time, trends in governance and within the context of a neoliberalist political paradigm make it attractive to shift responsibility towards individuals *as a governance arrangement*, which may happen precisely because existing governance structures have become hollowed out and fragmented. Governance arrangements are defined by Delemarle and Larédo (2014, p. 160) as "the constellation of arenas and their dynamics […] that are aligned in a robust manner." Giving individuals control over their own situation may be seen as an incentive for them to improve their position. This governance arrangement has been termed "responsibilization" (Eckhardt & Dobscha, 2018; Giesler & Veresiu, 2014; O'Malley 1996; Shamir, 2008) and can be defined as "a process whereby subjects are rendered individually responsible for a task which previously would have been the duty of another—usually a state agency—or would not have been recognized as a responsibility at all" (Juhila, Raitakari, & Hansen Löfstrand, 2019).

Responsibilization may also work as an arrangement when dealing with risks of new technologies. In these more individualized governance regimes, responsibility for uncertainty is attributed to different actors. Key roles are reserved for two actor groups. On one side of the spectrum, there are the technology developers, who as part of corporate social responsibility endeavor to create new knowledge about risks as they develop the market and exploit new technologies (Dorbeck-Jung & Shelley-Egan, 2013). On the other side of the spectrum, an equally important role is left to individual consumers. Individual consumers, through their consuming behavior, are "expected to address a wide variety of social issues through their individual consumption choices" (Eckhardt & Dobscha, 2018, p. 1).

Risk Personalization

When the governance landscape is fragmented, and/or suitable governance arrangements are not yet in place, allocating responsibility for risk decisions to individuals may seem an acceptable solution. Individual users of technologies make choices about how, when and where they use technology, and seem in a key position to assess and observe the impact of those choices with regard to their individual risk over time. In other words, responsibilization could be considered a feasible risk governance arrangement under conditions of uncertainty and fragmentation, which explains the connection between the abovementioned developments. With responsibilization, more individual responsibility is the *purpose* of risk governance.

In a general setting which emphasizes individual responsibility, however, leaving decisions to individuals may also happen *without* explicit responsibilization arrangements, and thereby also lack of consideration of alternatives. In those cases, individual responsibility may for example be the consequence of legal frameworks,

lack of collective decisions, etc. The externalities that collective forms of risk governance were meant to tackle can (re)appear in such situations. The aggregated decisions of those individuals may then lead to (new) collective risks. It is those developments that the risk personalization lens aims to uncover.

Three Cases of Risk Personalization

In this section, three cases of risk personalization are presented and subsequently analysed to illustrate and explore risk personalization in practice. A diverse set of cases encompassing different risk domains (physical and environmental safety, security) and governance arrangements (strong vs. weak) are selected. The case studies are small and descriptive and serve to illustrate "different characteristics of a phenomenon in its context" to allow for exploration of the risk personalization concept (Baškarada, 2014, p. 4). All three cases show how individuals via their role as consumers are expected to manage individual risks and also end up (intendedly or unintendedly) managing collective risks. The cases generate information about the governance of technology use and risk management under these conditions. In all three cases, there exists a collective risk resulting from individual technology use, where there is uncertainty about the governance of those risks and lack of clarity about who governs them, while at the same time the responsibility for the governance is placed at the level of the individual consumer/user. It should be emphasized that the case studies do not necessarily seek to represent the full extent of risk personalization and its implications, but merely to show the value of this concept under diverse governance settings and regarding different technologies.

Social Media and Privacy Waivers

Since 2005, there have been several social media platforms in use, with Facebook, Instagram, and WeChat as the biggest, connecting billions of people worldwide. At first glance, platforms such as Facebook and Instagram seem nothing more than public places for social networking, exchange of information and communication. And like other public spaces, risks to privacy are prevalent in the ethical and public debates about these platforms (Weir, Toolan, & Smeed, 2011). Apart from serious crimes such as identity theft, issues covered include risks of being refused a job based on social network pictures, or location data being used for unwanted purposes. These emerge because of design weaknesses that give unauthorized parties (hackers) access to the data, but also because of legitimate use of the associated services by both other users (checking social network sites of applicants) and by the service providers (using the data acquired for selective treatment of citizens).

Over time, ethical concerns over these platforms have moved beyond individual privacy (Anonimized). First, because users often do not only publish personal information about their own lives but also about the lives of their friends

and family. Second, the business models of most of these platforms lies in being able to predict what kind of person someone is (Hildebrandt, 2008), for example in order to show targeted advertisements or to decide who gets a loan and who does not. For such business models, the data of just one individual is useless; profiling data only make sense in the context of a broader population. When one possesses profiles of a large group, one can then make decisions based on those profiles, potentially leading to undesirable forms of bias and discrimination. Indeed, there is an accumulation issue: new risks emerge with increasing numbers of users supplying data. This has led some researchers to speak of a "tragedy of the privacy/data commons" (Fuchs, 2010; Yakowitz, 2011). Third, recent events around the intervention of Cambridge Analytica in the 2016 US presidential campaign shows that collective risk not only pertains to the commodification of personal information but that the large-scale accumulation of data also enables large-scale manipulation of voters on social media (The Guardian, 2018).

Furthermore, the governance landscape is fragmented. Increasing societal indignation puts pressure on (state) regulators and technology providers to provide consumers and societal actors such as governments and regulators more insight in the business practices of online platforms, and to counter online phenomena resulting from technology use such as targeted fake news. Privacy legislation, such as the EU General Data Protection Regulation (GDPR), creates new rules that govern the behavior of online providers, limiting for which purposes data can be used, and demanding individual consent as a form of choice architecture. Following the consent principle, the responsibility for governing the risks of data-release/sharing/storage is placed with individual users, via ex ante consent mechanisms and privacy waivers. Despite collective government arrangements, users are asked to check privacy agreements and privacy updates as they install and use social media platforms. These "solutions" have remained problematic. For example, individual users are unable to vary their use of media applications over time or based on the specific conditions they find themselves in. Thus, the options users are left with are either to opt-in or opt-out. In addition, although visibility of data to other users is often configurable, what cannot be selected is what data is shared with the social network provider itself.

Lastly, the choices imposed by the consent principle suggest that social media consumers are only dealing with *individual* risks, which could be managed through individual decisions. This goes back to privacy as the right to be left alone, informational privacy being one aspect of this (van den Hoven, Blaauw, Pieters, & Warnier, 2018). The market logic of a privacy waiver assumes that if individuals give explicit permission for the use of personal data by specific parties for specific purposes, then this shows that they must be ok with this arrangement. However, this individual waiver ignores shifting power balances through the large-scale gathering of data by certain players. Although individuals might be able to make decisions based on the consequences for themselves, the accumulation of power through data at the side of the service provider may not be factored in sufficiently in individual decisions. The uncertainty from a risk management perspective follows from the fact that it remains (relatively) obscure how platform companies use individual data as well as data obtained from others for other purposes.

Labeling of Nanomaterials in Cosmetics

Developments in fields like material science, chemistry, and physics have made it possible to produce nanoscale particles (1–100 nm). Nanomaterials are used in a variety of products and industries, such as cosmetics, foodstuffs, coatings, and construction materials (e.g., Cushen, Kerry, Morris, Cruz-Romero, & Cummins, 2012; Lee, Mahendra, & Alvarez, 2010). In cosmetics, nanomaterials are mostly used to improve product properties such as solubility and translucence. Examples of nanomaterials are nano titanium dioxide for producing transparent sunscreen, or nanosilver for its antibacterial effects.

However, experts are uncertain about the hazardous effects of such nanomaterials (Borm et al., 2006). There are indications that exposure to some nanomaterials may cause adverse health effects such as pulmonary diseases. It is known that nanomaterials may be easily taken up in the body after inhalation and ingestion. In addition to health risk, nanomaterial containing products may wash off and accumulate in the environment, though, release of nanomaterials from consumer products and solid composites have proven hard to model (Mackevica & Hansen, 2016).

The governance of nanomaterial use and production has been on the public and research[1] agenda of governments in western countries from early on. A proactive approach to risk regulation has been fed by sentiments living in the nano-sector to "avoid GMO like situation" (personal communication). In the European Union, the public debate on GMO has mandated a *de facto* moratorium on its use and consumption. Nonetheless, devising clear-cut risk regulation for nanomaterials is no easy task. Some argue that the Precautionary Principle should apply to nanomaterials (Van Broekhuizen & Reijnders, 2011), whereas others worry that too strict regulation may inhibit innovation. For years now, a debate takes place amongst specialists whether nanomaterials as a group of compounds actually warrants special treatment. "Nano" is not a label that indicates a level of hazard (such as irritants) or particular behavior (such as Persistent organic pollutants), the definition of nanomaterials used by the European union is foremost an indication of scale (European Commission, 2011),[2] a scale that may come with new properties and behaviors, but is not by definition hazardousness.[3]

In the wake of these discussions, the European Commission issued regulation that provides the legal contours for market access of cosmetics (Bowman, May, & Maynard, 2018).[4] These include requirements for the sharing of chemical and safety data, foreseeable exposure conditions, and ingredient listings in the Cosmetic Product Notification Portal. One of the rationales for this regulation was to increase transparency and information exchange about nanomaterials, in response to the so-called "information void" around nanomaterials (Bowman & Ludlow, 2009). The regulation obliges producers and importers of nanomaterial containing cosmetics to label nanomaterial content in their ingredient list by adding the word "nano" in brackets following the name of the substance. This is seen as a way of promoting transparency regarding the use of nanomaterials in cosmetics (Bowman et al., 2018) as it arranges the availability of information on nanocontent on the packages of several products to consumers.

The regulation also works to responsibilize individual consumers for the governance of uncertain nanomaterial risk. The regulation ensures that consumers have information about nanomaterial content in their products, thereby introducing a consumer choice that enables consumers to assess and decide whether they want to use a product that contains nanomaterials. This regulation has been criticized for being symbolic as known safety risks will always fall under the responsibility of producers. However, through this regulation the European Commission has also distributed responsibility over the cosmetics value chain, thereby allocating responsibilities for unknown and unquantifiable risk to consumers (Shelley-Egan & Bowman, 2015). Individual consumers may not easily fulfill these responsibilities, as most experts agree it requires additional testing and safety information to make fully informed choices.

Uber and Responsibility for Road Safety

Since its start in the early 2010s, the transportation network company Uber has been presented as the vanguard technological platform for the sharing economy heralding the end of the "traditional" mobility industry. Uber provides a platform for individual car owners to offer taxi services to Uber clients, without being part of the existing taxi business. From the onset, the legitimacy of Uber has been challenged, as it enables any individual owning a car to provide a service that is restricted in most countries to a specific group of providers (i.e., taxi companies) and/or professionals (taxi drivers). As such Uber has been disruptive: it provides a technology that breaks open the taxi industry and creates new competition (Cramer & Krueger, 2016). Competition that is not always deemed fair in a market with small margins which has left many taxi business owners vulnerable (Rushe, 2019; Sainato, 2019).

In addition to these concerns, questions have recently risen about the impact of Uber on road safety. For example, in the Netherlands, there was public outrage over an Uber driver who was involved in a deathly accident with a pedestrian (Van Bergeijk, 2018). Research has shown that "UberX drivers spend a significantly higher fraction of their time, and drive a substantially higher share of miles, with a passenger in their car than do taxi drivers" (Cramer & Krueger, 2016, p. 177). The Uber workforce is thus highly efficient in picking up new passengers. This has to do with the wide use and flexibility of the technology, the Uber-app effectively matches and connects drivers and passengers that are close by, and both drivers and passengers are incentivized to respond and connect supply and demand via dynamic pricing. To facilitate responsiveness, the Uber app actively monitors and steers driver behavior. Furthermore, Uber actively incentivizes driver behavior by introducing additional reward and badge systems for extra earnings and free college tuitions (Hawkins, 2018). These initiatives have been interpreted as ways to manipulate drivers into less attractive labor (e.g., at night or during holidays) using "video game techniques, graphics and noncash rewards of little value that can prod drivers into working longer and harder—and sometimes at hours and locations that are less lucrative for them" (Hawkins, 2018, p. 1). As Uber brings an inexperienced

and unregulated workforce on the streets, and actively nudges driver efficiency, the app may introduce road safety risks.

Road safety is not a new governance concern. What is new is that with Uber technology allegedly road behavior changes: a new group of drivers uses the roads more intensively, they have less experience, and their behavior behind the wheel is influenced and incentivized by technology to be responsive to instant pick-up demands, which may affect their alertness for traffic. Compared to the heavily regulated taxi sector, for Uber and its drivers, officially working independently, there are fewer governance arrangements. Several European countries have accepted and allowed Uber to operate, whereas others have experimented with and/or forbidden (forms of) Uber services.

However, regulatory arrangements for governing the use of the app have limitations. In many countries where Uber employs drivers, Uber is not formally based, and thus legally cannot be held accountable for conduct. As a result, the responsibility for the governance of road safety risks has become more fragmented; it lies at least partly with Uber drivers and end-users. Uber has vigorously claimed its app has technical features that stimulates safe driving.[5] For instance, it does not allow drivers to be logged in for more than a restricted number of consecutive hours. The company thus denies responsibility of stimulating individual "irresponsible" use even though it is part of the Uber business model that drivers continuously and actively engage with the app while driving, thereby distracting them. In the meantime, Uber drivers and users have only limited influence and options, primarily on the quality of one's own driving, and the choice to use or not use Uber.

Cross-Case Comparison

This section discusses the similarities and differences in the three different cases of risk personalization. We look at (i) the risk domain and sources of uncertainty, (ii) the governance arrangements, and (iii) the way in which emphasis is put on individual responsibility.

On Risks and Uncertainty

The three cases are situated in different risk domains (physical and environmental safety, and security risks), which all have different causes for uncertainty. In the nanomaterial case, the nature of risk is relatively straightforward. A physical material may or may not react with other physical materials and therefore pose (eco-) toxicological risks. In the social media case, collective risks emerge as a result of consumer and company behavior. Social media companies may or may not decide to profile and/or commodify personal data. Uncertainty has to do with a lack of knowledge about (future) company strategies and behavior, rather than not knowing physical properties, as is the case with nanomaterials. The cause of

uncertainty is indeterminacy rather than a lack of scientific information (Felt et al., 2007). In the Uber case, indeterminacy of the app and its effect, or rather the unpredictability of user/driver behavior can be identified. Furthermore, the interaction with other drivers, pedestrians, and road users adds another level of complexity to the issue which makes the influence of the technology on road safety (the actual risk the technology brings) hard to establish.

The discussed risks also scale differently. For the nanomaterial case, the accumulation of nanomaterials in the environment is of most concern and the risk usually grows incrementally until a threshold is reached and toxic effects occur. In the Uber case, the influence on road safety is imminent as soon as the behavior of at least some Uber drivers becomes risky. By contrast, in the social media case, the collective risk does not seem to exist until a critical mass of information is shared online, which paves the way for new kinds of analysis and business models for social media companies.

Furthermore, the cases vary with respect to whether the collective risks are easily observable for individual consumers. In the Uber case, one may argue that driving behavior of Uber users is directly visible to the Uber user and other road users, although obvious limitations in terms of alertness exist. However, there is the problem of connecting individual observations and obtaining insight in large-scale, more systemic patterns of driving behavior. In the case of nanomaterials, the risks are even harder to observe. The individual cosmetics user may read a product label but is not necessarily aware of other nanomaterials present in his/her environment. The individual user can therefore not accurately assess whether the accumulation of nanomaterials actually happens. In the social media case, the analysis of data collected from users and inner workings of social media companies are notoriously intransparent. It is unclear what kind of analyses are made and what is done to the data, and thus whether and to what extent collective risks may occur. Negative collective risks resulting from patterns and effects often only become visible only via in-depth analysis of multiple incidents, which resulted in scandals (e.g., Cambridge Analytica influences on US presidential elections). However, the (negative) collective effects of nudging and more subtle behavioral influences resulting from uncontrolled and intransparent behavior of companies remain undetected.

Governance Arrangement for Collective Risks

Governance responses to collective risk and uncertainty in these cases vary as well. For social media and Uber, the uncertainty remained unknown until evidence of collective risk emerged gradually over time; once the technology became more widely diffused, the potential negative effects became more visible, feeding concerns over a number of incidents, indicating a potential pattern. In-depth research, which identified and reported these effects, resulted in public outrage and demands for a governance response. In the nanomaterial case, uncertainties and collective risks were anticipated from the start by experts, as the physical risks of miniaturization and "tampering with nature" were foregrounded, and the need for some

form of governance arrangement to address collective risks was identified. This may have to do with nanomaterials being a paradigmatic example of an uncertainty and resulting risk that fits or at least seems to fit within existing risk management practices. However, the adequacy of the current governance arrangement in the form of product labeling is debatable.

In contrast to the nanomaterials case, in the social media and Uber cases, the need for governance arrangements was not immediately clear. Although nanomaterials carry associations with risk management of existing technologies such as nuclear power and GMOs, the emerging collective risks of digital platforms seem less well predictable, imaginable, or less threatening and only seem to be recognized in hindsight. In the meantime, the default personalized risk governance arrangement that allocates risk and the risk management responsibility to individual app users and Uber drivers is still in place pending resistance to change in the current governance arrangements.

The social media and Uber cases also demonstrate an asymmetry in capacity and resources to assess the (collective) risks resulting from new technology use. Governments are notoriously understaffed and lack important knowledge with respect to digital technologies. This information lag is reinforced by the notion that digital markets and tech companies are developing and evolving much faster than meaningful forms of regulation can respond. Furthermore, the cases point to an additional reason for the information asymmetry regarding public knowledge and data about collective risk(s): the strong link between the collective risk(s) and business models resulting from new technology use. The collective risk of profiling is not the result of a case of bad technology design, it is an essential feature of the current social media business model (and thus the result of deliberate technology design). Social media company revenues are primarily based on profiling, even though they portray themselves as platforms and enablers of communication to consumers. Uber does not profit from creating collective risks and safety hazards on roads *per se*. However, the Uber app does seem to directly affect driver behavior (looking at screens etc.) and not having that feature seems to dismiss the possibility of using the technology. Different app designs and incentives could in the future perhaps be developed to reduce collective risks.

The effectiveness of current individualized risk governance arrangements is thus questionable for different reasons. In the social media case, individual consent regarding privacy policies was put in place for digital technologies including social media, but many collective, societal risks resulting from social media use (e.g. fake news) have only recently been recognised. Profiling, commodification of data and associated manipulation are collective risks which have been identified but new governance arrangements have not (yet) been developed. These collective risks are seldom distinguished as typical problems resulting from large-scale use of social media and an inherent feature of the current business models that are sustained by the current governance arrangements. Uber had undertaken steps to improve road safety as a result of media coverage of complaints against the company. For instance, by developing features in their app to combat fatigue and make drivers more alert. However, whether the current risk personalization creates even more

dependency on an app that by itself may pose collective risks is the way to go forward in managing them could be debated. In the nano case, risk experts and product developers have failed to develop alternative governance arrangements despite decades of controversy and public debate. The current risk personalization regime assumes that individual consumers can solve the questions and problems that other actors in the value chain cannot.

Allocations of Responsibility to Individuals

The cases show different ways in which the responsibility to manage collective risk is allocated to individuals. In all three cases, one may argue, customers have a key choice: they can choose to (not) use the product or technology. In addition, in the social media case a choice is offered to mitigate individual privacy risks. However, the drawbacks of this risk governance regime are well-known (e.g., Bechmann, 2014). The current regime does not include the collective risk of profiling. If these need to be added, one could well argue that individual Internet users will be flustered with so many decisions that the rational approach is to "click them away". Users must decide to accept cookies for each website, a habit of ignoring the messages will develop quickly. This may even have a negative effect on consent decisions on other topics.

In nanomaterials the mechanism is different, it is assumed that by offering nano-labeling information to individual consumers, the result is an informed choice. However, this choice, if made actively, is rendered meaningless by the absence of clear scientific information about whether nano-materials in the product are actually dangerous. This may even promote collective scares, such as the ones who have been seen in the European debate about GMO governance (Knowles, Moody, & McEachern, 2007). In the Uber case, there is no clear moment of choice for individuals to pose questions or deal with the (collective) risk (just the choice to use the service). Responsibility for road safety falls by default (or by omission) on individual Uber drivers and other road users, which suggests that these actors and the current organization of responsibilities are able and sufficient to cope with all the problems that emerge from new technology use.

Summary of Cross-Case Comparison

The similarities and differences between the three cases that were discussed in this section help to understand more precisely what is at stake with risk personalization. Table 1 summarizes the cross-case comparison. Again, it is stressed that the overview is not meant as an exhaustive list. In the next section, we revisit the concept of risk personalization based on the theory and the cases.

Table 1. Cross-Case Comparison of Risk Personalization Cases

	Social Media	Nano	Uber
Source of uncertainty	Indeterminacy of company strategy (behavior) with regard to commodification of personal data (unknown unknown)	Indeterminacy resulting from lack of scientific information about physical properties of chemicals/products (known unknown)	Indeterminacy/ unpredictability of effect of technology (app) on user/driver behavior (and interaction with other road users) (unknown unknown)
Scaling of risk	Accumulation threshold (business model viability)	Accumulation threshold (assumption of linear, incremental risk curve)	Direct effect via app user (risk related to number of Uber drivers)
Observability of collective risk	Hidden from individuals, deliberate company intransparency obstructs monitoring of aggregation	Label only on individual level, nearly impossible to collect data to monitor aggregation	Observable on individual level, but difficulties in aggregation
Asymmetry in capacity and information due to:	Integral element of industry business model and governance arrangement	Lack of insight in aggregated individual assessments as a result of privacy rights of individual consumers	Other technology designs possible within current governance arrangement
Timeline of governance debate	Emerging, fed by empirical evidence	Apparent from the start	Emerging, fed by empirical evidence
Mechanism to allocate responsibility	Explicit consent for privacy arrangements	Labeling of nanocontent on product	Implicit as part of use

Discussion

This paper coined the concept *risk personalization* to start a conversation about a class of problems that emerges when the responsibility to govern uncertain collective risks is allocated to individuals. In present times, and against a background of fragmented governance, uncertain risks, and a general emphasis on individual responsibility, there are many instances of such allocation *outside* the explicit and purposeful arrangements of responsibilization.

Three diverse cases of risk personalization were analyzed to explore the phenomenon and its governance challenges. All cases represent individual responsibility in combination with aggregation of individual behavior into collective risk, while the cases differ in the risk domain and current governance arrangements. The conceptual lens of risk personalization helps to analyze how these cases vary in terms of the nature and scale of risks, some characterized by scientific uncertainty, and others by uncertainty about user and/or company behavior. Next, it identified variations in governance response to these risks, some emerging along the way and

others anticipating uncertainty and risk from the start. The cases showed big differences in terms of capacity and resources to govern these risks. In some cases institutions are formed; in the case of social media institutional voids (rather than failing institutional responses) could be identified. Lastly, the risk personalization concept facilitated reflection on the allocation or at least part of the responsibility to govern these risks to individuals. In some cases, risk personalization was enacted more actively, e.g. by explicitly providing individuals with a choice to mitigate or "manage risk" whereas in others the phenomena was more implicitly present, for instance because of the absence of other governance arrangements.

Governance Challenges

This study also shows that there are several governance challenges associated with risk personalization. A first governance challenge related to risk personalization is that the choices presented to individuals do not always present a conscious choice on the full extent of the collective risk. Even if it could be assumed that individuals could obtain all the appropriate information that would allow them to make informed decisions, it is not self-evident that their decisions would "add up" and result in a fair or adequate balance between individual and collective risks. In fact, for individuals, the risk personalization scheme offers possibilities and incentives to free ride and thus engage in individual use of new technology even though that could produce significant collective risks (such as giving away data for better service), whereas on a collective level these individual sacrifices aggregate to socially undesirable consequences, such as profiling-based discrimination.

A second governance challenge has to do with whether individual actions can meaningfully contribute by their actions to resolving or preventing these collective risks. Does it really matter what an individual posts in the face of millions of people sharing personal information online? Does it really matter that one individual uses a product that may pose a minute uncertain risk for the environment? With Uber this is clearer; it does matter directly that individuals drive safely. Furthermore, at what cost would individuals mitigate collective risks, especially if the individuals themselves are not exposed to them? In the case of Uber, one may not use the app as a driver. However, given that most Uber drivers do not use it as a side-job, as was intended by Uber, but as a main source of income, this is a choice with big consequences. Alternatives for some nanomaterials in cosmetics are available but may reduce functionality. There are technological alternatives for products like Facebook, but they do not provide the same social setting and interactions, precisely because almost everyone uses Facebook.

From the discussion above, it appears that the governance challenges in relation to risk personalization are mainly related to the "quality" of the choices made by individuals. That is, risk personalization only makes sense as a governance regime if the nature of the risk, as well as the way in which the choices are presented to individuals, allow for sufficient quality of the aggregated individual decisions with respect to addressing the collective risk. This is clearly not always the case.

The third governance challenge has to do with the design of the governance arrangement itself. Risk personalization is a "choice architecture" imposed on individuals (Thaler & Sunstein, 2008). This study shows that more sensitivity to the underlying reasons are for personalizing the risk governance in the first place might be useful. A set of questions could aid an analysis: Does somebody benefit from personalizing risk? If there are reasonable collective decisions to be made, why bother individuals? A lot of individual time and effort may be wasted if individuals are asked to make decisions that might as well have been made at a collective level. Moreover, collective decision making capacity may have value in itself, and this may be weakened if too many risk decisions are personalized. (The current pandemic is a good example of the value of collective decision making capacity.)

Policy Implications

Having identified all these challenges, does this mean that society should refrain from the personalization of risks of new technologies or that all risks should be governed via collective arrangements? Not necessarily. On the one hand, there are some roles that individuals can play in the governance of collective risk. For instance, when experts disagree about the existence and scope of risks as is the case with nanomaterials, it seems reasonable to ask individuals (as citizens or consumers) whether they would want to be exposed to these uncertain risks (as a form of informed consent). That would indeed imply that not only users, but also those facing externalities get a say in this. Furthermore, if the collective risk is at least partly manageable by individuals making changes to their behaviors, like in the Uber case, risk personalization could help to address them as responsible agents.

On the contrary, collective arrangements such as regulation and national policies, have their own limitations. To name but a few, governments have limited policymaking capacity. Centralized top-down policymaking is well-known for its many flaws and increasing inefficiency in today's complex society. Similar criticism is voiced against public regulation, which is always lagging behind, and public agencies may lack the information or expertise to identify the collective risks. A collective response may help to deal with new and emerging risks, but also obscure some of the complexities and difficulties surrounding them.

The key message is that risk personalization is the result of a choice (or the absence thereof) to distribute responsibility for the governance of uncertain collective risks in a particular way. A discussion about this arrangement and the tensions it brings needs to take place among stakeholders. Although tensions between collective risk and individual decisions have always existed, these tensions seem to increase as a result of governance arrangements in several domains. The explicit identification of risk personalization as a phenomenon enables a discussion about possible alternative governance arrangements, with the possibility of allocating responsibility at the level where decisions are most effective and efficient. This study thus aspires to have provided a lens that enables stakeholders to discuss about risk personalization.

Academic Implications

The risk personalization concept enables a sharper analysis and discussion about collective risks and their management resulting from the use of new technology. It facilitates a discussion about the distribution of responsibilities of actor groups and considers the limitations of decision making for *all* actor groups, including individuals. The collective consequences of individual use of technology and their connection to the way decisions about such risks are allocated to individuals as consumers are poorly understood and seldom explicitly addressed, and consequently remain largely remain outside already politicized debates about governance of these technologies.

Therefore, more research is needed on when and under what conditions risk personalization is an appropriate risk governance arrangement, and how it compares to other risk governance arrangements. For instance, does the way in which collective risks develop (e.g., via accumulation of individual behavior, the interaction between multiple processes, or via the behavior of a single actor or group) influence the effectiveness of individualized governance strategies? Does risk personalization lead to shirking, e.g. because corporations and governments shift their responsibilities to individuals? Risk personalization does not just happen, but follows from deliberate business case designs. What are the roles and responsibilities of intermediaries (e.g., platform and product development) that create and frame risk management choices?

With this paper, and the introduction of the risk personalization concept, discussions about the relationship between different actors such as governments, individuals, and collectives, in the governance of uncertain and collective risk are placed back on the research agenda.

Shannon Spruit, Department of Multi-Actor Systems, Delft University of Technology, Delft, the Netherlands [S.L.Spruit@tudelft.nl].
Mark de Bruijne, Department of Multi-Actor Systems, Delft University of Technology, Delft, the Netherlands.
Wolter Pieters, Department of Multi-Actor Systems, Delft University of Technology, Delft, the Netherlands.

Notes

1. http://www.oecd.org/env/ehs/nanosafety/.
2. A nanomaterial is "[a] natural, incidental or manufactured material containing particles, in an unbound state or as an aggregate or as an agglomerate and where, for 50% or more of the particles in the number size distribution, one or more external dimensions is in the size range 1–100 nm. […]" (European Commission, 2011).
3. Though, it seems the definition itself is stretched to include a wider range of particles to be subsumed under a stricter governance regime: "[…] In specific cases and where warranted by concerns for the environment, health, safety or competitiveness the number size distribution threshold of 50% may be replaced by a threshold between 1 and 50%."
4. European Cosmetics Regulation EC No. 1223/2009, on July 11, 2013.
5. See for example https://eng.uber.com/self-driving-telematics/.

References

Baškarada, Sasa. 2014. "Qualitative Case Studies Guidelines." *The Qualitative Report* 19 (40): 1–25.

Bechmann, Anja. 2014. "Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook." *Journal of Media Business Studies* 11 (1): 21–38. https://doi.org/10.1080/16522354.2014.11073574

Beck, Ulrich. 1992. *Risk Society. Towards a New Modernity*. London: SAGE Publications.

Bevir, Mark. 2012. *Governance: A very short introduction*. Oxford: Oxford University Press.

Borm, Paul J. A., David Robbins, Stephan Haubold, Thomas Kuhlbusch, Heinz Fissan, Ken Donaldson, and Roel Schins et al. 2006. "The Potential Risks of Nanomaterials: A Review Carried out for ECETOC." *Particle and Fibre Toxicology* 3 (1): 11. https://doi.org/10.1186/1743-8977-3-11

Bowman, Diana M., Nathaniel D. May, and Andrew D. Maynard. 2018. "Nanomaterials in Cosmetics: Regulatory Aspects." *Analysis of Cosmetic Products*, 2nd ed. 289–302. https://doi.org/10.1016/B978-0-444-63508-2.00012-6

Bowman, Diana M., and Karinne Ludlow. 2009. "Filling the Information Void: Using Public Registries as a Tool in Nanotechnologies Regulation." *Journal of Bioethical Inquiry* 6 (1): 25–36. https://doi.org/10.1007/s11673-009-9134-9

Cramer, Judd, and Alan B. Krueger. 2016. "Disruptive Change in the Taxi Business: The Case of Uber." *American Economic Review* 106 (5): 177–82. https://doi.org/10.1257/aer.p20161002

Cushen, M., J. Kerry, M. Morris, M. Cruz-Romero, and E. Cummins. 2012. "Nanotechnologies in the Food Industry—Recent Developments, Risks and Regulation." *Trends in Food Science & Technology* 24 (1): 30–46.

Delemarle, Aurélie, and Phillipe Larédo. 2014. "Governing Radical Change Through the Emergence of a Governance Arrangement." In *The governance of Socio-Technical Systems. Explaining Change*, eds. Borras Susana, and Jakob Edler. Cheltenham: Edward Elgar. 159–86.

Dorbeck-Jung, Bärbel, and Diana M. Bowman. 2017. "Regulatory Governance Approaches for Emerging Technologies." In *Embedding New Technologies Into Society. A Regulatory, Ethical and Societal Perspective (Chapter 3)*, eds. Diana M. Bowman, Elen Stokes, and Arie Rip. Singapore: Pan Stanford Publishing.

Dorbeck-Jung, Bärbel, and Clare Shelley-Egan. 2013. "Meta-Regulation and Nanotechnologies: The Challenge of Responsibilisation Within the European Commission's Code of Conduct for Responsible Nanosciences and Nanotechnologies Research." *Nanoethics* 7 (1): 55–68. https://doi.org/10.1007/s11569-013-0172-8

Eckhardt, Giana M., and Susan Dobscha. 2018. "The Consumer Experience of Responsibilization: The Case of Panera Cares." *Journal of Business Ethics*, 159, 1–13. https://doi.org/10.1007/s10551-018-3795-4

Ekberg, M. 2007. "The Parameters of the Risk Society: A Review and Exploration." *Current Sociology* 55 (3): 343–66. https://doi.org/10.1177/0011392107076080

European Commission. 2011. Commission Recommendation of 18 Oktober 2011 on the Definition of Nanomaterial Text with EEA Relevance. Brussels: European Commission. http://data.europa.eu/eli/reco/2011/696/oj

Felt, Ulricke, Brian Wynne, Michel Callon, Maria Eduarda Gonçalves, Sheila Jasanoff, Maria Jepsen, Pierre-Benoît Joly et al. 2007. *Taking European Knowledge Society Seriously. Report of the Expert Group on Science and Governance to the Science, Economy and Society Directorate*, Luxembourg: European Commission.

Fuchs, Christian. 2010. "Labor in Informational Capitalism and on the Internet." *The Information Society* 26 (3): 179–96. https://doi.org/10.1080/01972241003712215

Garland, David. 1996. "The limits of the sovereign state: strategies of crime control in contemporary society." *British Journal of Criminology* 36 (4): 445–71. https://doi.org/10.1093/oxfordjournals.bjc.a01410

Giddens, Anthony 1999. "Risk and Responsibility." *The Modern Law Review* 62 (1): 1–10.

Giesler, Markus, and Ela Veresiu. 2014. "Creating the Responsible Consumer: Moralistic Governance Regimes and Consumer Subjectivity." *Journal of Consumer Research* 41 (3): 840–57. https://doi.org/10.1086/677842

Hardin, Garrett. 1968. "The Tragedy of the Commons." *Science* 162 (3859): 1243–48. https://doi.org/10.1126/science.162.3859.1243

Harremoës, Poul, David Gee, Malcolm MacGarvin, Andrew Stirling, Jane Keys, Brian Wynne, and Sofia Guedes Vaz. 2001. *Late Lessons from Early Warnings: The Precautionary Principle 1896–2000*. Luxembourg: Office for Official Publications of the European Communities.

Hawkins, Andrew J. 2018. Uber Will Start Rewarding High-Performing Drivers with Better Earnings and Free College Tuition." *The Verge*. https://www.theverge.com/2018/11/1/18047746/uber-driver-high-performing-earnings-free-college-tuition-pro

Hildebrandt, Mireille. 2008. "Defining Profiling: A New Type of Knowledge?" In *Profiling the European Citizen*. Dordrecht: Springer Netherlands, 17–45. https://doi.org/10.1007/978-1-4020-6914-7_2

Hood, Christopher, Henry Rothstein, and Robert Baldwin. 2001. *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford: Oxford University Press.

Hutter, Bridget M. 2010. *Anticipating Risks and Organizing Risk Regulation*. Cambridge: Cambridge University Press.

Juhila, K., S. Raitakari, and C. Hansen Löfstrand. 2019. "Responsibilisation in Govermentality Literature." In *Responsibilisation at the Margins of Welfare Services*, eds. K. Juhila, S. Raitakari, and C. Hall. London: Routledge. 2017: 11–34. ISBN 978-1-138-92838-1.

Klinke, Andreas, and Ortwin Renn. 2012. "Adaptive and Integrative Governance on Risk and Uncertainty." *Journal of Risk Research* 15 (3): 273–92. https://doi.org/10.1080/13669877.2011.636838

Knowles, Tim, Richard Moody, and Morven G. McEachern. 2007. "European Food Scares and Their Impact on EU Food Policy." *British Food Journal* 109 (1): 43–67. https://doi.org/10.1108/00070700710718507

Kuhlicke, C. 2011. "Perspectives on Social Capacity Building for Natural Hazards: Outlining an Emerging Field of Research and Practice in Europe." *Environmental Science and Policy* 14: 804–14.

Lee, Jaesang, Shaily Mahendra, and Pedro J. J. Alvarez. 2010. "Nanomaterials in the Construction Industry: A Review of Their Applications and Environmental Health and Safety Considerations." *ACS Nano* 4 (7): 3580–90. https://doi.org/10.1021/nn100866w

Mackevica, Aiga, and Steffen Foss Hansen. 2016. "Release of Nanomaterials from Solid Nanocomposites and Consumer Exposure Assessment—A Forward-Looking Review." *Nanotoxicology* 10 (6): 641–53.

Mullin, Richard P. 2002. "What Can Be Learned from DuPont and the Freon Ban: A Case Study." *Journal of Business Ethics* 40: 207–18. https://doi.org/10.2307/25074882

O'Malley, Pat. 1996. "Risk and Responsibility." In *Foucault and Political Reason: Liberalism, Neo-Liberalism and Rationalities of Government*, eds. Andrew Barry, Thomas Osborne, and Nikolas Rose. London: Routledge. 189–207.

Renn, Ortwin, Andreas Klinke, and Marjolein Van Asselt. 2011. "Coping With Complexity, Uncertainty and Ambiguity in Risk Governance: A Synthesis." *Ambio* 40 (2): 231–46. https://doi.org/10.1007/s13280-010-0134-0

Renn, Ortwin, and Pia-Johanna Schweizer. 2009. "Inclusive Risk Governance: Concepts and Application to Environmental Policy Making." *Environmental Policy and Governance* 19 (3): 174–85. https://doi.org/10.1002/eet.507

Rhodes, Rod A. W. 1997. *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability*. Buckingham: Open University Press.

Rushe, Dominic. 2019. What Is Uber? Forget the Sharing Economy—It's Just a Libertarian Scam." *The Guardian*. https://www.theguardian.com/commentisfree/2019/may/09/uber-sharing-economy-ride-share-ipo

Sainato, Michael. 2019. "'They Treat Us like Crap': Uber Drivers Feel Poor and Powerless on Eve of IPO." *The Guardian*. https://www.theguardian.com/technology/2019/may/07/uber-drivers-feel-poor-powerless-ipo-looms

Seawright, Jason, and John Gerring. 2008. "Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options." *Political Research Quarterly* 61 (2): 294–308.

Shamir, Ronen. 2008. "The Age of Responsibilization: On Market-Embedded Morality." *Economy and Society* 37 (1): 1–19. https://doi.org/10.1080/03085140701760833

Shelley-Egan, Clare, and Diana M. Bowman. 2015. "The Challenge of Distributing Regulatory Responsibilities for Unknown Risks:'Nano'-Cosmetics and the EU Cosmetics Regulation as a Case Study." *Journal of Clinical Research & Bioethics* 6: 212–22.

Taleb, Nassim N. 2008. *The Black Swan: The Impact of the Highly Improbable*. London: Penguin.

Thaler, Richard, and Cass Sunstein. 2008. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. New Haven, CT: Yale University Press.

The Guardian. 2018. "Cambridge Analytica's US Election Work May Violate Law, Legal Complaint Argues." https://www.theguardian.com/uk-news/2018/mar/26/cambridge-analytica-trump-campaign-us-election-laws

Van Bergeijk, Jeroen. 2018. "An Uber-Driver Kills a Young Woman and Uber, Her Parents Conclude, 'Does Nothing at All' (Een Uber-Chauffeur Rijdt Een Jonge Vrouw Dood En Uber, Stellen Haar Ouders Vast, 'Doet Daar Helemaal Niets Mee')." De Volkskrant.

Van Broekhuizen, Pieter, and L. Reijnders. 2011. "Building Blocks for a Precautionary Approach to the Use of Nanomaterials: Positions Taken by Trade Unions and Environmental NGO's in the European Nanotechnologies Debate." *Risk Analysis* 31 (10): 1646–57.

van den Hoven, Jeroen, Martijn Blaauw, Wolter Pieters, and Martijn Warnier. 2018. ""Privacy and Information Technology." In *Stanford Encyclopedia of Philosophy*." In *Metaphysics Research Lab*, ed. Edward N. Zalta. Stanford: Stanford University. Summer 201.

van Waarden, Frans. 2001. "Institutions and Innovation: The Legal Environment of Innovating Firms." *Organization Studies* 22 (5): 765–95.

Weir, George R. S., Fergus Toolan, and Duncan Smeed. 2011. "The Threats of Social Networking: Old Wine in New Bottles?" *Information Security Technical Report* 16 (2): 38–43. https://doi.org/10.1016/j.istr.2011.09.008

Wiener, J. 2010. "Risk Regulation and Governance Institutions." In Risk and Regulatory Policy Improving the Governance or Risk. Paris: OECD Publishing. 133–57. https://doi.org/10.1787/9789264082939-en

WRR Scientific Council for Government Policy. 2009. *Uncertain Safety. Allocating Responsibilities for Safety*. Amsterdam: Amsterdam University Press.

Yakowitz, Jane. 2011. "Tragedy of the Data Commons." *Harvard Journal of Law & Technology* 25 (1): 1–67.