Data Pollution and Taxation

Gertsen, Fred

DATA POLLUTION AND TAXATION

by

Fred Gertsen

Executive Master Cyber Security: Thesis

Student Number: s1358693

Date submitted: March 10, 2022
Date defended: March 31, 2022

Table of Contents

Abstract

Data sharing and data harvesting practices not only infringe the privacy rights of individuals but cause significant harms to others as well. Emissions of personally sensitive behavioural data are leaked into the digital economy causing damage to social practices and destabilizing political and informational ecosystems. Data pollution is like industrial pollution, and environmental law suggestions can offer solutions to the problem. Will a Pigouvian tax on data extraction limit or constrain the negative externalities of data pollution? This explorative research aims to investigate whether a data pollution tax can operate as a regulatory instrument to curb data pollution and whether citizens support this measure. Do citizens support a data pollution tax designed so that harms to others, affecting their core human capabilities, will be taxed as a matter of principle? Suppose excessive (corporate) data sharing and extraction practices that cause harm to others will be taxed. Do individuals expect that persons and corporations will change their data transmission practices? Our survey findings show that (United States) citizens consider that harms caused by data pollution should be taxed. Respondents will also substantially decrease their data pollution behaviour once a tax is imposed. However, and to our surprise, our research findings also lay bare a possible 'bad behaviour paradox': the more significant the harm caused by some instances of data pollution, the less willing people are to change behaviour relative to the tax imposed.

1 Introduction

1.1 Data Pollution, Key Concept and Research Objectives

Digital data transmissions and extraction has created many positive attributes and values for individuals, the economy, and society. These positive effects of digitalization on personal life and financial wealth have been documented by numerous authors (Carlsson, 2004; Lammi & Pantzar, 2019; Myovella, Karacuka, & Haucap, 2020; Sutherland & Jarrahi, 2018). Also, the positive contribution of the digital economy, and the impact of digitization on improving productivity and innovation, has been well documented (Kroll, Horvat, & Jäger, 2018; Van Ark, 2015). Moreover, the proliferation of using the internet, and the related ascent of digital platforms, has significantly contributed to the efficient and effective usage of otherwise idle assets (Codagnone & Martens, 2016; Fraiberger & Sundararajan, 2017).

However, next to these positive effects of the data economy, there are also significant adverse effects of the data sharing and harvesting practices. Collecting personal behavioural data by digital platforms, either with or without consent, not just harms the privacy interests of the individuals concerned but also creates significant negative externalities to other individuals, groups, and society, as documented by Acemoglu, Makhdoumi, Malekian, and Ozdaglar (2019); Acquisti, Taylor, and Wagman (2016); Bergemann, Bonatti, and Gan (2019); Couldry and Mejias (2019); Zuboff (2019a). Besides, with their dominant market positions and monopolistic powers, digital platforms create significant negative externalities to groups of individuals and society. These developments have been well documented by the Stigler Committee of The University of Chicago on Digital Platforms (Zingales, 2019).

The concept of 'data pollution', coined by Ben-Shahar (2019)[1], endeavours to convert the one-dimensional, individual-privacy-only view of regulation concerning data harvesting, data protection and privacy concerns. The data pollution concept provides an original perspective that explains why regulatory mechanisms currently fail to prevent social harms caused by excessive data sharing and harvesting practices. Next, the ever-increasing power of digital platforms needs to be remediated. Notably, Couldry and Mejias (2019) qualify platforms' power as 'data colonialism, West (2019) terms it 'data capitalism', and Zuboff (2019b) calls it Surveillance Capitalism. The data pollution concept proposes, how and why alternative regulatory instruments need developing to limit the harms of behaviour modification, caused by these excessive data sharing and extraction practices. Taxation of data pollution, the subject of this thesis, could be a regulatory or legal measure to limit these

[1] Ben-Shahar, O. (2019). Data Pollution. *Journal of Legal Analysis, 11*, 104-159.

extreme data practices and thereby decrease harms caused to others (other individuals or groups of individuals).

1.2 Data Extraction Causes Harms to Others, at Individual and Group Level

This thesis will argue that next to the effects of data pollution on public goods (harms to the social and political environment and informational ecosystems), data pollution also impacts the more intangible individual and collective assets of core human capabilities. How technology affects human capabilities was first conceptually developed by Sen (2001) and Nussbaum (2011) in their 'Capabilities Approach'. Scholars investigating data colonialism (Couldry & Mejias, 2019; Mejias & Couldry, 2019) also connect this Capabilities Approach with data justice (Couldry, 2019).

Currently, giving consent to sharing data has become a meaningless 'click', as is well documented by Ben-Shahar and Schneider (2014); Solove (2012). Therefore, should data harvesting practices be restricted by behavioural data extraction limits, such as quantitative limits, data emission permits and quota? Alternatively, should 'behavioural-change feedback loops' trigger real-time corrective measures by, for example, warning data polluters of excessive data extractions with high pollution characteristics? Or should data pollution emissions be taxed based on the value of the (aggregate) positive or negative externalities they create? Regulatory advantages and disadvantages of these various data pollution regulatory control measures were evaluated by Ben-Shahar (2019), Thimmesch (2016), and more recently, Babcock (2021).

Some initiatives were taken to create value awareness amongst data sharing individuals. Illustrative for these initiatives is the 'Ernie App', which builds on the premise of individuals' 'Right to Monetize' their data sharing practices. Data subjects are not sufficiently aware that they create value with their data sharing activities, and the Right to Monetize intends to adjust this situation.[2] The concepts of 'Data Dividends', developed by the Berggruen Institute (Feygin et al., 2021) under 'The Data Dividends Initiative', and supported by the Governor of California, also considers that data sharing by individuals should be compensated fairly.

Before discussing data pollution tax as a possible regulatory solution, a brief review of other data-tax related issues will be identified based on current literature (Cockfield, Hellerstein, & Lamensch, 2019; Cui, 2019; Köthenbürger, 2020; Marian, 2021). After that, a taxonomy of data pollution harms will be used to investigate whether a so-called Pigouvian tax (Jacobs & De Mooij, 2015; Marian, 2021) is considered an appropriate regulatory measure to ensure that the negative externalities caused by data pollution harms are internalized. This absorption of harms can include individuals sharing data and corporate pollution actors. If a data pollution tax would be imposed on

[2] Right to Monetize, see https://ernieapp.com/privacy-is-a-right-the-right-to-choose/

data sharing practices that damage human well-being, would data polluters decrease their data polluting activities?

This explorative research aims to investigate whether a data pollution tax has the potential to operate as a regulatory instrument to curb data pollution and whether citizens support this measure. Do citizens support a data pollution tax designed so that harms to others, affecting their core human capabilities, will be taxed as a matter of principle? Following on from this, if excessive (corporate) data sharing and extraction practices, which harm the integrity of 'self' and others will be taxed, do individuals expect that individuals and corporations will change their data transmission practices? These measures according to Couldry and Mejias (2019, pp. 167 - 172) could limit the relatively high cost of data pollution harm to society.

1.3 Research Questions

This study aims to operationalize the data pollution concept by assessing harms caused to others' well-being and whether these data sharing activities can be decreased by raising a tax on these activities. Main research question: Should data pollution be taxed?
Research Sub-Questions:

I. Which harms to others are caused by data pollution?
II. Can data pollution activities be categorized into individual cases and corporate cases?
III. Based on the literature of harms caused by data pollution, can a taxonomy of harms be developed to assess intangible damages affecting core human capabilities?
IV. Do citizens want to tax data pollution based on the level of harm caused by intangible harms? Does 'intent to share data' have an impact on the level of taxation?
V. If a data pollution tax is levied, based on harms caused and intent to share, do individuals expect data polluters to change their data sharing and harvesting practices? Does imposing a data pollution tax affect pollution behaviour elasticity?

1.4 Theoretical Framework and Development of Hypotheses

We will provide an overview of data pollution as a concept that has recently become a domain of study of various academic disciplines. Like its sister concept of environmental pollution, data pollution can be studied from a sociological, political, economic, and regulatory perspective. Another approach would be to assess the effects of data pollution from a physical perspective; in line with environmental concerns, how do the exponential growth of data sharing, data storage, and the necessary equipment and energy use (server farms) contribute to physical pollution. However, the core research topic of this thesis is how data pollution causes harm to human well-being and whether these pollution activities can be restrained by levying a tax. Our research methodology will therefore comprise three fundamental components.

Firstly, Chapter 2, will review the generic literature on data pollution. Starting with the article of Ben-Shahar (2019), we will trace back the development of the concept of data pollution to earlier academic studies. Secondly, as we want to develop a survey that considers the various forms of some current data pollution cases, we will carry out an in-depth review of the academic literature of data pollution instances. The review will serve as the basis for developing data pollution vignettes. This literature review will guide the iterative process of vignette development. At the same time, we will endeavour to find generic characteristics of data pollution cases, such as technological affordances and other addictive features of data sharing applications. Together, these findings will guide the vignette construction. Thirdly, in Chapter 3, we will use information from the literature review to develop our research model and related hypotheses.

1.5 Methodology, Results and Findings

In Chapter 4, Methods, we will describe how we will test our hypotheses by deploying a survey tool (Qualtrics) designed to run through CloudResearch[3] and Amazon Mechanical Turk (Litman & Robinson, 2020). Various challenges have been identified in running questionnaires on Amazon Mechanical Turk (MTurk), and potential issues on research effectiveness will be addressed. The number of questions in the survey will be limited and will be based on the following:

1. Questions on the necessity to impose a data pollution tax to curb data pollution transmissions.
2. Questions on qualitative/quantitative assertions that query: should data pollution that affects aggregate core human well-being dimensions of others be taxed? Using a limited number of vignettes that describe pollution harms to others, the responder will be queried on the extent to which specific human capabilities are affected negatively and how much tax should be levied based on overall harm.
3. A question on the perceived intent to share data that affects others.

[3] For CloudResearch, see https://www.cloudresearch.com

4. Does the responder expect a change in data sharing/extraction behaviour of the pollution (vignette) actors if a tax is levied? Next, will responders change their data sharing behaviour if a tax is imposed?
5. The questionnaire will be designed to explore whether a correlation exists between various data pollution harms, their severity, the preferred pollution tax rate, and the anticipated decrease in data transmission if a tax is imposed.
6. Additional questions will cover political orientation, gender, age, ethnicity, education level, and survey participation ethics.

We will run statistical mediation analyses and other statistical tests that will inspect the hypotheses based on the survey results. Chapter 5 will contain a summary of those results and Chapter 6 will interpret significant findings of this study and will also include some suggestions for future research.

1.6 Limitations of Research

Academic works on negative externalities of data extraction are clustered into academic silos. This diversification of research into various academic fields was identified by de Brouwer (2020, p. 10) and Humbert, Trubert, and Huguenin (2019). The data pollution phenomenon is often rephrased, or named differently, depending on the academic domain it is being considered in. Studies on surveillance capitalism (Zuboff, 2019a), digital surveillance (Y. Park, 2021), the platform society and its effects on being human (de Reuver, Sørensen, & Basole, 2018; DeVito, Birnholtz, & Hancock, 2017; Evans, 2012; Fenwick, McCahery, & Vermeulen, 2019), or behaviour modification, all share theoretical connections with the current study. However, this thesis limits its investigation to data pollution, by addressing the question whether individuals recognize various forms of data pollution. Additionally, we will investigate how they assess intangible harms of data pollution, and whether individuals believe that taxation of data sharing activities will limit the data sharing behaviour. Do citizens have an appetite for a data pollution tax and will the elasticity of demand of data sharing be affected by this additional tax penalty?

We also limit our survey to respondents in the United States of America (US). The main reason for this being that the questions on taxation levels are expressed in US Dollars and are tailored to monthly average costs of an internet subscription in the US.

2 Theoretical Framework - Data Pollution and Negative Externalities

2.1 Proliferation of Data Collection Practices and Tangible Harms

Data sharing practices by individuals, and data harvesting by corporations raise concerns with academics, regulators, politicians, and society for a variety of reasons. Firstly, there is concern that our global demand for, and growth in physical data processing capabilities, will lead to unprecedented levels of energy consumption. Next, the underlying and exponentially growing communication ecosystems, including the internet of Things, will cause an ecological footprint of massive scale. E-waste and extraction of rare earth elements cause damaging e-footprints (Bakhiyi, Gravel, Ceballos, Flynn, & Zayed, 2018)

In *Reset*, Deibert, the founder of the Citizen Lab writes: 'Our consumption of social media (and the communications ecosystem that supports them) generates a kind of hidden tax on the natural environment…' 'They are contributing to massive environmental degradation' (Deibert, 2020, p. 210). Hidden externalities of our growing communications ecosystem, have an ecological footprint of massive scale. There are more tangible reasons to consider. Data server farms are expected to consume 10% of our electricity capacity by 2025 and this is expected to increase thereafter. Exponentially growing communication ecosystems, including the IoT and soon, the so-called 'Metaverse' (a combination of virtual reality, augmented reality, and the internet), will contribute to the massive ecological footprint. E-waste and extraction of rare earth elements cause e-footprints. Currently, we create 60 zettabytes of data, growing to some 200 zettabytes by 2025. By 2035 expectations are that we create more than 2000 zettabytes (Morgan, 2020) , which would cost some $60 trillion or about 40% of global GNP to store data. These unprecedented data storage requirements will have use implications for energy consumption and will have potentially disastrous effects on the physical and economic climate of planet Earth (Bietti & Vatanparast, 2020).

However, next to these tangible physical pollution effects of surveillance capitalism and data colonialism, there are also substantial intangible effects of extensive data harvesting practices that impair human autonomy, agency, privacy, dignity, and well-being. That will be the topic of the next section.

2.2 Intangible Data Pollution Effects and Negative Externalities

Information shared by, and extracted from people affects others, and it undermines and degrades public goods and interests (Ben-Shahar, 2019, pp. 106 - 107). External harms to other individuals and groups (and the public) originate from *intentional* release of personal data (Facebook release for political ads - case), but also from *unintentional* release through data breaches (for example Equifax). In his article 'Data Pollution', Ben-Shahar (2019, p. 118) argues that harms caused by data extraction are currently addressed mainly from the perspective of injuries to individual privacy. He provides convincing evidence that individual and corporate data sharing practices within the data economy also create negative externalities that cause harm to other individuals and groups (Ben-Shahar, 2019, p. 108).

Data pollution is not the aggregate harm of privacy harms (or other harms) to groups of individuals, nor is it derivative damage of distrusting corporations, platforms, or governmental institutions. Rather, at group level, it is direct and tangible or intangible harm to public ecosystems (also called neighbourhood effects or spill overs). Data is hazardous and can get toxic when sensitive data (or its imputed correlatives) is dispersed into data processing ecosystems. Data pollution as defined by Ben-Shahar is a social problem. In economics, the concept of externalities is used to identify cost or benefits that are caused by a producer, but which cost are not incurred, or benefits do not accrue, to that producer. These externalities, however, do impact third parties that are affected by the producer. A good example is industrial pollution causing harms to the environment. With respect to data pollution, in principle two externalities can be considered (Avraham, 2018). The first is that individually shared data can be used and aggregated and affects public interests. The second externality arises when users not only share their own data, but also share information of others and affect others at a group level. The collective of individuals, the 'computed group' is potentially harmed, which is different from the sum of effects at individual level. This is in line with de Brouwer (2020, p. 10), when he writes '…when the issue is systemic and the externalities accumulate'.

Hirsch and King (2016), and more foundational Hirsch (2006), consider the negative externalities of big data to be like environmental pollution. Earlier, Schneier (2015, p. 279), in his book *Data and Goliath*, referred to data pollution in more restrictive terms, as follows: '…data is the pollution problem of the information age, and protecting privacy is the environmental challenge.' The data pollution concept of Ben-Shahar provides an innovative, more inclusive, and promising theoretical background for addressing harms caused to others by data sharing and extraction practices.

In a recent interview with the New York Times[4], Shoshana Zuboff, author of *Surveillance Capitalism*, explains the importance for privacy of limiting cross-application, and cross device tracking. Users of digital media applications are often unaware of the data sharing attributes of the applications they use and how these applications affect others. Next, the willingness to share

[4] *The New York Times* (May 21, 2021), Shoshana Zuboff interviewed by Lauren Jackson, see https://www.nytimes.com/2021/05/21/technology/shoshana-zuboff-apple-google-privacy.html?action=click&module=Features&pgtype=Homepage

personal data with close or distant recipients also shows that data privacy is a complex process of trading off costs and benefits (Schudy & Utikal, 2017). Finally, and which makes data pollution very difficult to resolve, there is social media's persuasive powers and addictive nature. The unrelenting requirements of giving consent to contractual demands, have caused a 'privacy fatigue' (H. Choi, Park, & Jung, 2018), and online apathy regarding privacy (Hargittai & Marwick, 2016), accelerating data pollution and its negative externalities.

Unlike environmental pollution, which has been around for some 150 years, data pollution as a phenomenon, has a much shorter history of perhaps some 25 years. Unfortunately, it took society a considerable time to recognize and act on the disastrous effects that environmental pollution has on well-being of societies and our planet. The effects of data pollution have perhaps also been underestimated; this study attempts to create academic awareness on this topic by operationalizing the concept of data pollution and its potential taxation.

Not long ago, both in an article for *The New York Times*[5] and in an academic publication, Twenge et al. (2021) concluded that most research on the mental health effects of social media consumption addresses how the individual consumer is affected. The authors believe this to be inadequate as social media consumption has changed peer relationships, transformed family bonds, and has changed how people interact in conversations: social media affects social groups and cohesion. Substantiating the notion that data pollution is considered a recent phenomenon, of interest is that the term information pollution was first used by Jakob Nielsen in 2003 to describe irrelevant, redundant, unsolicited, and low-value information (Nielsen, 2003).

The concept of data pollution includes information pollution or 'infollution' (Özdemir, 2016), as coined by Oram 1984. However, information pollution is different to some extent; 'the contamination of information sources with irrelevant, redundant, unsolicited and low-value information' or as Cai and Zhang (1996) quote: '… is a pile of widespread yet unwanted messages and that one day, these messages could deeply influence the social life bearing negative results.' Our focus in this study is on data pollution: my data sharing (or that of corporates) affects others.

2.3 Theory on Generic Characteristics and Issues of Data Pollution

Like environmental pollution, data pollution can be caused by a variety of actors, either intentionally (hackers, data breaches) or unintentional (data hungry apps, unintentional disclosure by others). The economics of the digital society are based on the paradigm that digital users share as much data as possible to enable the extraction of behavioural surplus data that can be monetized by the big data

[5] *The New York Times*, Opinion and Guest Essay by Jonathan Haidt and Jean M. Twenge (July 31, 2021): This Is Our Chance to Pull Teenagers Out of the Smartphone Trap.

platforms and its supply chain. These extensive data sharing and data harvesting practices lead to negative externalities that have not yet been specifically addressed in literature.

How does this extensive data sharing industry create negative impacts on individuals, groups, and society? ‘An externality exists whenever the welfare of some agent (individual, household or firm) depends not only on his or her activities, but also depends on activities exercised and under control of some other agent’ (Tietenberg & Lewis, 2018). Reflections on how privacy of individuals and privacy as a member of a group, has extended the concept of privacy harms, and has led to various clusters of research (de Brouwer, 2019, 2020) on both an abstract privacy level (group privacy, interrelated privacy) studied in various academic disciplines, and to more detailed studies on major occurrences (types, categories) of data pollution.

Moreover, in a recent publication, de Brouwer (2020, pp. 3, 10) lists separate literature clusters that address data pollution variants, or approach the negative externalities of the data pollution phenomenon from a particular theoretical point of view. Key elements de Brouwer refers to are privacy infringements and externalities caused by third parties, the collective (group) dimensions and elements of privacy, interdependent aspects of privacy and its infringements, and the inferential nature of current technologies. The following extensive quote from de Brouwer illustrates the wide variety of academic research into the extended privacy concept. Quoted from de Brouwer (2020, p. 3):

> *‘…joint controllership*, and *privacy infringements* (Helberger and van Hoboken, 2010; van Alsenoy, 2015; Edwards et al., 2019) or *infringements of data protection law* and *networked services* (Mahieu et al., 2019); *collective privacy* (Squicciarini et al., 2009) and *collective action problems in privacy law* (Strahilevitz, 2010); *multi-party privacy* (Thomas et al., 2010); *collateral damage* and *spillover* (Hull et al., 2011; Symeonidis et al., 2016); *interpersonal management of disclosure* (Lampinen et al., 2011); *networked privacy* (boyd, 2011; Lampinen, 2015; Marwick and boyd, 2014); *interdependent privacy* (Biczók and Chia, 2013; Symeonidis et al., 2016; Pu and Grossklags, 2017; Kamleitner and Mitchell, 2019); *peer privacy* (Chen et al., 2015; Ozdemir et al., 2017); *multiple subjects personal data* (Gnesi et al., 2014); *privacy leak factor*, *shadow proLles* and *online privacy as a collective phenome-non* (Sarigol et al., 2014); *privacy externalities* (Laudon, 1996, pp. 14-6; MacCarthy, 2011; Humbert et al., 2015, 2020; Symeonidis et al., 2016; Choi et al., 2019), especially as compared to externalities in the context of environmental pollution (Hirsch, 2006, 2014; Hirsch and King, 2016; Froomkin, 2015; Nehf, 2003; Ben-Shahar, 2019); 1 *genetic groups* (Hallinan and De Hert, 2017); or *sociogenetic risks* (May, 2018)’

The concept of data pollution is closely related to the concept of information pollution, and its subsets of misinformation, disinformation and mal-information, see Wardle and Derakhshan (2017). Information pollution is concerned more with how false or harmful information, either intentionally or accidentally, misleads individuals, groups, or information ecosystems. If information consists of 'data with contextual meaning', then information pollution is a subset of data pollution.

Currently, harm from data releases and extraction only evaluate harms to personal privacy, including a person's well-being, autonomy, dignity and equality (Schwartz & Peifer, 2017). However, harms from data misuse are greater than the sum of all private injuries. Data misappropriation creates public harms and destroys public goods. As is clearly evidenced by the Cambridge Analytica incident, damage is caused to electoral and political ecosystems. Information ecosystems need to be protected from data sharing contracts, not just the individual data providers.

Preceding Ben-Shahar's paper on data pollution, other authors identified negative externalities of data sharing to other individuals and at group level. Acemoglu et al. (2019) describe that Bergemann et al. (2019); J. P. Choi, Doh-Shin, and Byung-Cheol (2019); Fairfield and Engel (2015); MacCarthy (2010), are the first studies that concentrate on the externalities of data sharing. Additionally, Jin (2019) has written on how AI affects consumer privacy.

MacCarthy (2010) was one of the first authors to argue that negativities of data leakage, originating in data mining practices and in social media networks, cannot be prevented through the legal instrument of individual consent. Referring to earlier work by Solove (2004), MacCarthy argues that regulation of the usage of consented data should be considered as a solution to the negative externalities of data harvesting, not the collection of data itself. Recently, Acemoglu et al. (2019) also underwrite this concern and propose to prevent harms by regulating data usage. MacCarthy also points to the negative inferential potential of non-disclosure of information. For example: non-smokers have an incentive to report their good lifestyles to health insurance companies (lower premiums), thereby potentially identifying and harming smokers that remain silent on their unhealthy habits.

Following MacCarthy, Fairfield and Engel (2015) also argue that privacy should be considered as a 'public good', or rather, in quite a few instances, as a 'public bad'. Mining big data collections to illuminate patterns, Fairfield et al. argue, can lead to behavioural or informational inferences on aspects of a person's life that she did not want to reveal, or she was unaware of owning. In many instances, a person is kept in the dark on how group data inferences impact her well-being, either financial or non-financial. For example, paying higher insurance premium that results from being part of a family or group of friends (with certain health or behavioural characteristics they privately shared) is not transparent to the non-disclosing party, but causes her financial harm, nevertheless.

Finally, J. P. Choi et al. (2019) also recognize how data controllers can take advantage of an individual's data disclosure to draw inferences about others who refrain from disclosure. They refer to other studies that document these negative externalities: 'Facebook Likes' that predict undisclosed sensitive personality traits, genetic tests drawing inferences on groups, and adverse selection predispositions by insurers related to tracking driving behaviour, see also Wachter and Mittelstadt (2019) on the rights of individuals to 'reasonable inferences'.

Recently, more attention is paid to the effects of individual data harvesting on group identification. Often unknown to the data provider, algorithms are used to calculate, to which 'calculated publics' (Gillespie, 2014) an individual can be assigned, manipulated and nudged, in order to predict or influence behaviour. Group privacy, defined as the privacy belonging to the group as a separate entity, and not as the sum of its members, provides many new insights in how data harvesting creates economic harms, both at those group levels and for the individuals 'assigned' to the group. The concept of group privacy, coined by Taylor, Floridi, and Van der Sloot (2016), creates new legal challenges as well. Currently, legal paradigms on privacy are primarily focused on how privacy breaches harm the individual. How these affordances relate to controlling privacy, see Trepte (2020).

Ben-Shahar's data pollution concept also sheds some light on the so-called 'privacy paradox' (Athey, Catalini, & Tucker, 2017; Hargittai & Marwick, 2016; Norberg, Horne, & Horne, 2007). The paradox: individuals assert that they are worried about their privacy online; however, their apparent careless online behaviour contradicts these concerns. The 'right to be left alone' as framed initially by Brandeis and Warren (1890), more than one hundred years ago, needs reconsideration when applied to the group level. When individuals share data, and consequently impair their own privacy, the privacy of individuals whose information is either associated (family, friends etc.) or correlated (algorithmic groups), gets compromised at the same time (Christakis & Fowler, 2009).

The resulting negative externalities lead to an avalanche of data sharing practices. Individuals, taking into consideration what is already known about them through information shared by others, de-value their own information and privacy. Therefore, inefficiency arises when a subset of users is willing to release its data freely and which data is about other users, whose value of privacy is high.

Acemoglu et al. (2019) provide evidence that the price of a person's data decreases when others leak information about that individual. The Cambridge Analytica scandal presents substantive evidence of this group data externality: based on private information of some 270.000 Facebook users, Cambridge Analytica was able to create behavioural inferences of more than 50 million Facebook users. The volunteered information of the few can unlock the same information about the many, see also Barocas and Levy (2020).

Privacy has been framed in terms of protecting the individual (Maldoff & Tene, 2019, p. 53) and the power to manipulate individuals, groups and society based on their data, lies with corporates and governments, not only with individuals (N. M. Richards & Hartzog, 2020). The fiduciary model of privacy argues that as we entrust data controllers with our sensitive personal data, they should be assigned with having a fiduciary responsibility in processing the data (Balkin, 2020; N. Richards & Hartzog, 2016). In this thesis we will be able to compare data pollution behaviour at an individual level (harms, intent to harm, tax level and behavioural change) with data pollution behaviour at corporate level.

2.4 Theory on Specific Pollution Mechanisms and Negative Externalities

2.4.1 Data Pollution Components

What is data pollution? Within the context of environmental pollution, we intuitively understand pollution to be 'the introduction of contaminants into the natural environment that causes adverse change (or harms) to the environment'[6]. Before we can define the mechanisms and characteristics of what constitutes 'data pollution' we will consider some determinate aspects of environmental pollution. As documented by Springer (1977), pollution is an important concept in environmental law, and is used in many international agreements, such as the 1972 'Stockholm Declaration on the Human Environment'. The Springer (1977) article is of interest to this thesis as the author articulates criteria that signify when a threshold of legal significance regarding environmental pollution is exceeded; Springer discusses various past (legal) approaches to the concept of pollution, of which the following three are of particular interest: pollution as damage, pollution as interference with other uses of the environment, and finally, pollution as exceeding the assimilative capacity of the environment. Springer articulates that the pollution concept contains two important characteristics of cause and effect: a spreading mechanism (contamination, contagion, cascading, spiralling, amplification, etc.), and a harm effect to an ecosystem.

To be able to speak of 'pollution damage', there must be 'injury of health or property on the other'. In numerous cases and countries, courts have addressed what qualifies as pollution damage. They established legislation, regulation, and heuristics to determine when pollution damage is either substantial, serious, carries sufficient evidence, and whether inconvenience or discomfort should be considered.

[6] Pollution defined in Wikipedia: https://en.wikipedia.org/wiki/Pollution

On 'damage to the environment', concepts of 'harmful contamination', 'adverse changes', 'unfavourable alteration' are of relevance. Interference with other use of the environment can be critiqued for disregarding the interdependent biological characteristics of ecological systems (Dunn, 2021). Finally, whether ecosystems can assimilate the pollutants without disturbing the fragile equilibria, has become an important aspect of the definition of pollution.

The polluting mechanisms underlying data pollution (and/or information pollution)[7] need to be defined. What are key characteristics or similarities in data sharing (extraction) ecosystem practices that would qualify these practices as 'polluting'? Which negative effects on an ecosystem as a whole, at an organismic, holistic, and self-organizing level, would justify qualifying a phenomenon as pollution, thereby not just focusing on pollution damage to its parts or segments (Capra & Luisi, 2014)? Following Boley and Chang (2007), we assert that affecting an ecosystem through pollution, there needs to be some form of 'multiplication' involved that harms a healthy (harmonious and sustainable) state of an ecosystem and exacerbates potential damage.

The next paragraphs (2.4.2 through 2.4.10), organized around a limited number of data pollution cases, will elicit from academic literature some of the major contamination, contagion, and spreading mechanisms, prevalent in data sharing practices, ultimately causing data pollution harms. Attention will also be paid to common attributes of these pollution mechanisms. These attributes (enablers), we suspect, are the technological affordances that facilitate the 'easy to use', and effortless spreading mechanisms (Withagen, De Poel, Araújo, & Pepping, 2012). Affordances have also been linked with addiction in on-line gaming (Lee, Cheung, & Chan, 2021) and social media addiction (Dwyer & Fraser, 2016). Next, affordances have also been associated with more negative aspects of persuasive technologies, such as addictive behaviour and other psychological stressors (Fox & Moreland, 2015; Hamari, Koivisto, & Pakkanen, 2014).

These affordances not only explain how the pollution mechanisms are set in motion, but the affordances could also be of influence on how the intent of spreading or sharing data are a determinant of possible changes in behaviour. Perceived intent to share will be an important factor in determining whether taxation of data pollution will lead to a change in data sharing behaviour given the assessment of harms caused by that data pollution.

As will further be explained in Chapter 3, we developed data pollution vignettes using an iterative process between a review of theory (next paragraphs), consideration of recent media disclosures on data pollution (e.g*., The Wall Street Journal Facebook Files*[8]), and choices regarding

---

[7] We consider information pollution to be a subset of data pollution. Information to be defined as 'data with meaning'; see (Mingers, 1995), Information and Meaning.
[8] The Wall Street Journal Facebook Files (2021), see https://www.wsj.com/articles/the-facebook-files-11631713039

the impact pollution has on others. The next table on pollution vignettes provides an overview of nine individual pollution cases and their corporate counterparts.

The following table shows how the individual vignettes link with the corporate vignettes:

Table Vignette Themes:

Nr I/C	Vignette Theme	Section Reference	Name Individual Vignette (I)	Name Corporate Vignette (C)
1 / 11	Data Sharing Affordances	2.4.2	Layla	TELROT
2 / 12	Location Sharing	2.4.3	Julia	SEYU
3 / 13	Disinformation Spreading	2.4.4	Dany	CAMLITE
4 / 14	Hate Speech Dissemination	2.4.5	Thierry	CLOCKO
5 / 15	DNA Data Sharing	2.4.6	Carlo	PHARAX
6 / 16	Data Breaches	2.4.7	Robin	CREDO
7 / 17	Sharing Sensitive Data	2.4.8	Ashley	GRAY
8 / 18	Data Surveillance	2.4.9	Sabrina	GOOGLE
9 / 19	Photo and Video Sharing	2.4.10	Shane	TRESSOR

2.4.2 Data Sharing Affordances

Many social media systems have incorporated a system of technological affordances, such as 'like, share, comment, thumps, kudo's', that can be qualified as feedback loops with characteristics of reinforcing spirals, as documented by Boers, Afzali, Newton, and Conrod (2019); Slater (2007). The relationship between technological affordances and addictive behaviours has been documented by (Dwyer & Fraser, 2016). Based on a review of articles on how usage of social network sites related to body image disorders, and combined with findings from 'social comparison theory', Holland and Tiggemann (2016), Tiggemann, Hayden, Brown, and Veldhuis (2018) conclude that these social network sites contain a mechanism that perpetuates existing social prejudice regarding body image.

Moreover, social contagion theory (Christakis & Fowler, 2013) explains how seeking positive feedback through 'likes', and comparable instruments, becomes addictive and leads to compulsory connective behaviour on social media sites (Dumas, Maxwell-Smith, Tremblay, Litt, & Ellis, 2020). The contagious nature of social comparison in social media systems has been further documented by S. Choi and Kim (2020), de Vries, Möller, Wieringa, Eigenraam, and Hamelink (2018), and also by Feinstein et al. (2013). Emotion and morality loaded messages on Twitter have been found to cause twenty percent more diffusion in the social media network (Brady, Wills, Jost, Tucker, & Van Bavel, 2017).

Furthermore, third-party trackers are built into so-called 'data-hungry' apps that leak user's personal information to data brokers and even to unknown (Brandtzaeg, Pultier, & Moen, 2019; Egele, Kruegel, Kirda, & Vigna, 2011; Van Kleek et al., 2017). Claesson and Bjorstad (2020) document how private and sensitive information of users is shared by friends and others without the user's consent or awareness. On-line diffusion, made possible by technological affordances, has structural characteristics that mimic the spreading of infectious diseases. The expression 'going viral' (Goel, Anderson, Hofman, & Watts, 2016) illustrates how affordances significantly contribute to contagious behaviours.

Recently reported on by *The New York Times*[9], and subject of academic research, the spreading effects of networks' own misinformation labelling practices (YouTube and Twitter's warning labels), provide evidence of the contagious nature of misinformation sharing between networks (Buntain, Bonneau, Nagler, & Tucker, 2021; Pierri, Piccardi, & Ceri, 2020; Sanderson, Brown, Bonneau, Nagler, & Tucker, 2021).

2.4.3 Location Data Sharing

Individual users of fitness tracking devices share location data that, when combined with data of other users, contributes to the creation of location heatmaps that can cause harm to others (Ben-Shahar, 2019, p. 113). Apps using location data (Strava, Fitbit, etc.) apply persuasive gamification and competitiveness features that encourage users to change behaviour and to share their data with many others, often beyond family, relatives and close friends (Barratt, 2017). Motivational affordances built into the Strava app, entice users to interact with other Strava users (Rivers, 2020). These affordances are designed to satisfy a core human desire to experience interaction with other humans, leading to social bonding (Ryan & Deci, 2000). Combining these affordances with features of gamification, passionate competitiveness, and peer pressure, fitness apps, and Strava in particular, fuel the engine of social contagion, leading to sharing physical activity performance and sensitive location information (Rowe, Ngwenyama, & Richet, 2020; Whelan & Clohessy, 2020).

Location and contact tracking, based on mobile apps, has become a major topic for health authorities and governments around the globe due to the Covid-19 pandemic (T. Sharma & Bashir, 2020). Due to the networked nature and multiple layer hierarchy in contact tracing, these location-

[9] *The New York Times* (October 14, 2021), YouTube's stronger election misinformation policies had a spillover effect on Twitter and Facebook, see https://www.nytimes.com/2021/10/14/technology/distortions-youtube-policies.html

based apps imply a multiplication factor congruent with its network properties (Li, Zhu, Du, Liang, & Shen, 2016). However, also before the pandemic, US Federal Agencies and the IRS (Internal Revenue Services) acquired location data to detect undocumented immigrants and locate criminals involved in tax schemes (Tau, 2020; Tau & Hackman, 2020) . As further disclosed after publication of the Snowden Papers (Bauman et al., 2014; Landau, 2013), government authorities throughout the world contract the private sector to enhance the profiles they keep on citizens who have not consented to sharing their location data. These ubiquitous surveillance practices lead to significant privacy issues (Caminker, 2019) and to privacy pollution, as formulated by Froomkin (2015). Unrestricted location tracking can also lead to significant national security risks as was documented by *The New York Times* in 2019 (Thomson & Warzel, 2019).

2.4.4 Disinformation Spreading and Amplification Mechanisms

The speed and scale of spreading disinformation in volume, reach, and velocity, is principally facilitated by the open ‘connective’ nature of the internet. The mechanism of retweeting activities has significantly contributed to the dissemination of false information content (Meel & Vishwakarma, 2020). Additionally, engagement with news, and subsequent sharing of news information through social media, is influenced by the interplay of technological affordances of social media networks and human factors, including heuristics and biases (S. Park, Sang, Jung, & Stroud, 2021, pp. 1010 - 1011). Researchers have addressed tweeting behaviour, information diffusion patterns, detection system-abilities (Laaksonen, Haapoja, Kinnunen, Nelimarkka, & Pöyhtäri, 2020), all shedding light on the origin, dispersion, detection, and intervention of polluted (false) information . Analyses of the polarization effects of reinforcing information spirals through Facebook’s news algorithm has been extensively documented (Beam, Hutchens, & Hmielowski, 2018; Del Vicario et al., 2016). Platforms’ destabilizing effects on media ecosystems (Wardle & Derakhshan, 2017) and, more recently, its related editorial challenges, has been documented by Donovan and Boyd (2021) in historical context.

Interestingly, several authors have found that false information spreads significantly faster, wider, and deeper into networks compared to true content (Lavorgna, 2021, p. 46 (kindle); Lazer et al., 2018, p. 1095; Vosoughi, Roy, & Aral, 2018, p. 3). Other authors (Ferrara, Cresci, & Luceri, 2020, p. 272), qualify this undisciplined proliferation of fake news and misleading information as ‘infodemics’, which in case of the current pandemic can have deadly consequences.

The presidential elections of 2016 in the United States also boosted the number of ‘fake news’ studies (Allcott & Gentzkow, 2017; Guess, Nyhan, & Reifler, 2018). These studies show that exposure to fake news is strongly associated with predetermined conservative information needs and that misinformation campaigns bear more fruit with the less educated. In a recent opinion article in *The New York Times*[10], and based on the work of Bail et al. (2018), Michelle Goldberg refers to social media as 'the engines for spreading disinformation and jet fuel for conspiracy theories'. False information on the Coronavirus has already resulted in harm to physical well-being, and even death, as documented in recent research (Mian & Khan, 2020; Tasnim, Hossain, & Mazumder, 2020).

Based on analyses of Twitter data in crisis circumstances, Hui, Tyshchuk, Wallace, Magdon-Ismail, and Goldberg (2012) call the mechanism of Twitter users propagating information to a large audience, 'information cascades'. The multiplication characteristics of information cascades (Cheng, Adamic, Dow, Kleinberg, & Leskovec, 2014; Dow, Adamic, & Friggeri, 2013) and its domino effect have been documented comprehensively (Jalili & Perc, 2017; Mizrahi, 2020).

2.4.5 Hate Speech Dissemination

Hate speech, through its widespread dissemination, advances a vision of society that accepts intolerance and discrimination. Speech-acts involving hate speech not only causes discriminative harm to others, but their performative nature constitutes harm in itself (Barendt, 2019). The public good of ascertaining protection against discrimination is undermined for individuals being part of that group. The source itself is multiplicative as its 'performativity' affects all members of groups directly (Simpson, 2013, p. 6). Hate speech, through its widespread dissemination, advances a vision of society that accepts intolerance and discrimination. The pollution is not caused by one single hate speech-act. Instead, the impact of the assemblage of technological affordances and messages (Ben-David & Fernández, 2016, pp. 1168 - 1171) pollutes and affects the equilibrium of social ecosystems. Trolling, the internet practice of posting insincere, digressive, and inflammatory messages, to evoke emotional responses, often elicits strong multiple responses (Cheng, Bernstein, Danescu-Niculescu-Mizil, & Leskovec, 2017; Phillips, 2019). Trolling has been attributed to an 'Internet Culture' in which irony, lulz (fun and laughter), and false innocence are used as excuses for deviant behaviour (Phillips & Milner, 2021). Trolling behaviour has also been associated with the 'Dark Triad' personality disorder framework, which explains its manipulative and contaminative intentions (Craker & March, 2016).

The amplification and circulation of messages through 'likes, comments, and share' buttons are examples of covert discriminatory practices (Ben-David & Fernández, 2016, p. 1187). The affordance of cross-postings also contributes to the ease of spreading both text and images in hate speech networks (Pearce et al., 2020). For affordances that enable cyberbullying, see Chan, Cheung,

[10] Opinion *The New York Times*, November 1, 2021, by Michelle Goldberg: We should all know less about each other. For The Polarization Lab at Duke University (Chris Bail), see: https://www.polarizationlab.com

and Wong (2019). A documentary on social media and Alt-Right demonstrates how technology design contributes to the acceleration of hate speech (Lindquist & Hermansson, 2018). Cloaked websites, hiding the origins of authorship and disguising its political agenda, also contribute to cyber-racism and its spreading mechanisms (Daniels, 2009).

The elaborative use of hashtags (#) is another affordance used in disseminating hate speech through social media networks (Skaza & Blais, 2017). Racialized hashtags, so-called 'Black-tags', are used to amplify existing discriminatory practices online (S. Sharma, 2013). Hate speech has a higher spreading velocity through social networks than other messages and attracts a larger audience at a faster than regular rate (Mathew, Dutt, Goyal, & Mukherjee, 2019). Spreading mechanisms of hate speech related to particular groups are also illustrative of its contagious and epidemic nature (Ferrara, 2017, p. 6; Zannettou, Finkelstein, Bradlyn, & Blackburn, 2020, pp. 786, 796). Information cascades and how networks diffuse power to different actors, also support the notion that 'hate speech systems' contain robust multiplier characteristics (Jalili & Perc, 2017; Masud et al., 2021).

2.4.6 DNA Data Sharing Affecting Others

With the advent of direct-to-consumer genetic testing, users of social media networks often disclose their genetic test results publicly, spreading genetic data more profound into the public domain (Olejnik, Kutrowska, & Castelluccia, 2014). When individuals share genetic data, information about others, by definition, is disclosed as well (Baig, Mohamed, Theus, & Chiasson, 2020); *re*production is a process of copying, hence affects others. Individuals who have family ties or share genetic codes are possibly affected by additional disclosures of DNA related diseases or other heritage-related predictive parameters concerning present or future physical, psychological, and potentially social attributes. Suppose assemblages of genetic groups map onto recognized social groups (called genetic classes vs genetic categories). In that case, the additional social 'identities' will lead to other concerns regarding segmentation, sorting, and signalling (Hallinan & De Hert, 2017, p. 176).

Additionally, the affordances available in heritage apps increase the ability to target, extract, and share information with individuals genetically related (Turrini, 2018, p. 8). Moreover, databases containing DNA information are often shared with unrelated commercial third parties (Baig et al., 2020).

2.4.7 Data Breaches and Sharing Personally Identifiable Information

Leaking of crawled data exacerbates data breach harms due to the size and interpretation potential of crawled data. Web crawling and scraping (also called bots, spiders, and crawlers) were traditionally used to automatically index data of websites, enabling search engines to scan, analyse and store information of websites systematically. However, these crawlers and scrapers can also feed information content underlying the index into algorithms and inference engines. The collection of scraped raw data enables the analysis and interpretation at a higher meaning-making level, not anticipated or consented to by the raw data originators, giving rise to ethical and legal concerns (Gold & Latonero, 2017, p. 278). Web crawlers are not subject to laws and regulations and, by their nature, constitute an ever-present surveillance mechanism, collecting, processing, and storing data of web users. Corporations, researchers, and government authorities extensively use web crawling, including law enforcement and police (Gold & Latonero, 2017, p. 283).

Data breaches at the victim side can be associated with device affordances. For example, a user's habits and heuristics of his mobile device can cause phishing attacks to succeed (Vishwanath, 2016).

2.4.8 Online Dating Applications

Creating profiles on dating sites involves disclosing highly sensitive personal information to the 'outside' world, such as sexual preferences or substance use history (Cobb & Kohno, 2017), linking a user's social and non-dating media networks through cross-platform data-sharing affordances (Albury, Burgess, Light, Race, & Wilken, 2017). By constantly sharing geolocation, this data sharing exposes the information of friends and relatives (Murphy, 2017, p. 104; Ostheimer & Iqbal, 2019, p. 3), enabling digital stalking. The reciprocity of sharing sensitive data through dating apps, combined with algorithmic intent to exploit, enables the data industry to maximize revenues from data of others (MacCarthy, 2010).

Unfortunately, and implicating other app users, Grindr shared HIV related data and location data of its users, as documented by Ghorayshi and Ray (2018); Warner, Gutmann, Sasse, and Blandford (2018). These authors share similar privacy and safety concerns, expressed by Claesson and Bjorstad (2020); Myrstad and Tjøstheim (2021); sharing sensitive personal information without consent creates significant privacy breaches for others.

Contrary to these data breaches, in dating-app ecosystems, authorized users cause harm to other users by intentionally violating trust or by re-identifying users through their profiles and data from other apps. For example, taking screenshots from dating apps and sharing them with friends, or uploading the screenshots to social media, can cause private information to go viral (Cobb & Kohno, 2017, p. 7). The flip-side of sexual harassment through dating apps is discursive activism in which feminist groups publicize dating app misuse through, again, viral mechanisms in social media (Shaw, 2016). Dating apps create sophisticated instruments for 'geodemographic profiling' to segment and sort users and make correlational inferences about them. These data pools are shared with and are valuable to data brokers (Albury et al., 2017, p. 5) and cause significant well-being harms to others.

2.4.9 Data Surveillance and Extraction

Google collects data of Gmail recipients, not being Gmail users (and vice versa) without their consent[11] and sells this information to data brokers and the US National Security Agency (NSA) for mass surveillance (Rushe, 2013). Google's massive data collection and profiling practices and how those practices affect non-Google users has been the subject of litigation (Batiste-Boykin, 2015; "Google Inc. Gmail Litigation," 2013). When we share personal information, we also provide access to knowledge about others who do not share their information. These spillover effects of an individual's data sharing (Tucker, 2019) and related externalities have been documented by J. P. Choi et al. (2019) and MacCarthy (2010). As N. M. Richards (2012, p. 1937) describes in *The Dangers of Surveillance*, '… surveillance is systematic; it is intentional rather than random or arbitrary'; and: '… surveillance is routine - a part of ordinary administrative apparatus…'.

Research indicates that individuals disclose more personal information through web forms than strictly necessary for the application at hand (Krol & Preibusch, 2016; Preibusch, Krol, & Beresford, 2013). More recently, mobile apps are a significant source of revealing personal data to third-party trackers (Binns et al., 2018; Van Kleek et al., 2017). Studies show that data collected through mobile apps are shared with unknown recipients and are exchanged contractually with specific third-parties (Egele et al., 2011; Jinyan Zang, 2015). These apps allow data brokers to access private information for credit scoring, payment apps (Brandtzaeg et al., 2019), and other surveillance purposes. Binns et al. (2018) illustrates the pervasive nature of third-party tracking arrangements that exist in news apps and apps targeting children

Moreover, surveillance derives its value from pattern recognition of data on individuals concerning others and groups. Continuous monitoring and algorithmic connection and inference mechanisms cause surveillance to be a perpetual data collection engine. Shoshana Zuboff has written persuasively on the systemic accumulating logic that underlies the surveillance capitalism mechanisms of Google and Facebook. She argues that once: '…data flows have been labelled by technologists as "data exhaust", … their extraction and eventual monetization are less likely to be contested' (Zuboff, 2015, p. 79). Extraction is a one-way process, not a relationship - it is a 'taking from'. Once data extraction has led to a genuine commercial transaction, the cycle of monetizing

[11] See also details on Electronic Privacy Information Center (EPIC) for further details (par 2.3): https://epic.org/privacy/gmail/faq.html#23

surveillance data assets begins again (Zuboff, 2015, p. 80); surveillance has thus become a never-ending data extraction and accumulation mechanism.

2.4.10 Photo and Video Sharing

Sharing images of self and others through social media networks has increased with Web 2.0 and the affordances of image capture by mobile devices. Banal life is now on exposé (Ibrahim, 2015), and next to ordinary life, image sharing is currently one of the essential features of social network sites (Malik, Dhir, & Nieminen, 2016).

However, next to the multiplication in real life, it has also led to a surge in academic interests on how images distributed through social media affects many aspects of culture and society (Yan Chen, Sherren, Smit, & Lee, 2021). Shared and tagged pictures expose the emotions of others without their consent. Other authors have addressed how the affordances of sharing and uploading photos in Facebook strongly contribute to rumour cascading by measuring replication strength and longevity of message instances (Dow et al., 2013; Friggeri, Adamic, Eckles, & Cheng, 2014; Yim, Malefyt, & Khuntia, 2021).

2.5 Conclusion on Theory, Supporting the Concept of Data Pollution

Various forms of data sharing and extraction practices have significantly increased during the past ten years, as illustrated above in Chapter 2. In this chapter, as also documented by de Brouwer (2020, p. 3), we reviewed literature from various academic disciplines that researched some of the critical characteristics of data pollution: firstly, how technological affordances cause amplification, secondly, how these affordances lead to addictive data sharing behaviours, and, finally, how many of these compulsory data sharing activities cause harms to others. In the next Chapter 3, and more specifically in paragraph 3.3, we will develop discuss how five key harms of data pollution cause harm to others' human well-being. Additionally, we will construct a research model that enables us to develop hypotheses to test whether a data pollution tax will lead to data polluters changing their behaviour causing harm to others.

3 From Theory on Data Pollution to Research Design

3.1 Using Data Pollution Vignettes

The previous chapter provides an overview of some significant instances of data sharing and data extraction practices that, based on the harms they cause to others, can be qualified as data pollution cases, following the theoretical underpinnings provided by Ben-Shahar (2019); de Brouwer (2020). Unfortunately, the negative externalities of these practices, and their potential harms on the well-being of others, have only recently been conceptualized as a pollution issue comparable to environmental pollution. This study aims to operationalize the data pollution concept by assessing harms caused to the well-being of others and whether these data sharing activities can be decreased (limited) by raising a tax on these activities.

However, as became evident in the theoretical part of this study, data pollution is a 'container concept' and exists in many disguises. We believe that by using survey vignettes we will be able to convey to survey respondents the characteristics of data pollution (Alexander & Becker, 1978; Atzmüller & Steiner, 2010). Moreover, it will create a basis to clarify its potentially damaging effects on other data subjects, groups, society, and information ecosystems.

Consequently, an iteration process evolved between conceptualizing various data pollution cases and their theoretical substantiation utilizing our literature study. The validity of the vignettes as cases of realistic data pollution has further been corroborated by the 'first cluster' literature review on 'general' data pollution issues (Chapter 2.3).

Each vignette contains a short and carefully constructed description of various data pollution instances. These data pollution instances, or cases, all share several pollution characteristics in a variety of assemblages, as summarized in the following paragraph. We shall also provide some more theoretical grounding for the definitional elements of data pollution that we considered in drawing up the data pollution vignettes. The following generic and descriptive items are used in these vignettes: data sharing format, the utilization of specific affordances that enable data sharing, and implications of data sharing on others (possible cause of harm).

During this iterative process of identifying data pollution instances, we noted that next to individuals causing data pollution, also corporations massively engage in data extraction and data sharing practices and thereby inflict harm to others. For each case of data pollution, we were able to find similar pollution cases in which corporations appear to be the leading actor. For example, sharing location data through Strava (individual case) resembles, to an extent, the sharing (and commercial exploitation) of location data by telecommunication providers (see vignette 2/12). Another example of pollution case 'pairing' is genetic test data sharing on an individual level (vignette 5) and DNA-test companies selling genetic data to pharmaceuticals for advertising purposes (vignette 15). Our literature review in Chapter 2, and our work on constructing data pollution vignettes confirms the validity of our research sub-question (II): 'Can data pollution activities be categorized into individual cases and corporate cases? On that basis, our hypotheses will differentiate between individual and corporate instances of data pollution.

3.2 Defining Data Pollution

According to de Brouwer (2020, p. 3), data pollution can occur through the following mechanisms[12], with potential effects at either individual or group level:

a) When a person directly discloses information about another individual (blogging, allowing Facebook or Strava[13] to access friends' lists).
b) When aggregation of individual data at group level causes harms to others.
c) When data reveals a person by indiscriminate capture of information of a group (event recordings with images, sound, and location data). Similarly, whether at group level, inferences can be made about location data and associations (or inferences) with others.
d) Instances where relational data between individuals is disclosed (genetic data, household, and neighbourhood data).
e) Non-causal inferences of specific characteristics based on big data correlations (calculated publics, non-disclosure of negative traits), see also (Solow-Niederman, 2021; Wachter & Mittelstadt, 2019).

During the development of data pollution vignettes and based on the theory described in Chapter 2, the criteria described below were used to assess whether the data sharing and extraction practices described in the vignettes would qualify as data pollution instances. In summary, data pollution and negative privacy externalities occur if the following criteria are met:

- Sharing data of others: The contractual consideration (or 'price') for a digital service not only consists of sharing the user's data but also contains data of others. Includes data contagion mechanisms and data crawling.
- No consent: The consent by one data subject to share data, impacts other data subjects and pre-empts their consent.

[12] Based on, and adapted from de Brouwer (2019), Privacy Self-Management and the Issue of Privacy Externalities (Thesis, Utrecht University)
[13] For illustration, see the Strava heatmap of Kabul in Ben-Shahar (2019, p. 113)

- Others benefit: Data sharers or data controllers benefit to the (potential or actual) detriment of 'third-party' data subjects. Others cause 'my data' to be exploited and monetized. My data serves as raw material.
- Impairs human well-being: Impairs elements of ADEPS[14] (five dimensions of well-being). A cost (including intangible, non-monetary harms) is imposed by the data sharer, or data controller, on third party data subjects.
- Others cause inferences: Others sharing data on me generate algorithmic (correlational) assumptions that are false and cause harm to me and others.
- Harms to ecosystems/public goods: The injuries caused (negative externalities) are often abstract with, in some instances, no actual direct harm to the individual. These externalities undermine and degrade public goods.

The characteristics of data pollution mentioned above, were used to develop, and structure the contents of the data pollution vignettes. In the next paragraph we will develop our primary hypotheses on how these data pollution instances generate intangible harm to others.

3.3 Intangible Harms and Effects on Human Capabilities

The literature on harms (Chapter 2) caused by various data sharing and extraction practices shows a wide variety of damages. These harms extend from group privacy harm to tangible financial damages of algorithmically inferred and calculated groups. How do the externalities, as mentioned earlier, both at individual and group levels, relate to human capabilities?

Acquisti et al. (2016) conclude that due to increasing information asymmetries, consumers are not well-positioned to make reasoned decisions about sharing private data, and whether data sharing harms themselves or others. These authors also recognize that information economics and its analyses of costs, harms, and benefits is an assemblage of various fields of study. However, they make specific reference to Schoeman (1992, p. 133) on how data sharing practices can have implications for human dignity, autonomy and freedom. They also mention that the value consumers assign to their personal data is difficult to pinpoint (see the earlier discussion on the Privacy Paradox). More recently, various academics (Floridi, 2016; Frischmann & Selinger, 2018; Zuboff, 2019a) and also 'grey literature' (Kool, Timmer, Royakkers, & van Est, 2017) make specific reference on how participation in the digital world creates exposures on core value dimensions of

[14] Harm Dimensions (5): Privacy (P), Autonomy (A), Safety and Security (S), Human Dignity (D), Equity and Equality (E),

being human. Next to privacy, they include concerns on human agency, autonomy, dignity, equality, power, and self-directedness.

In 2017, the Dutch Rathenau Institute[15] issued a report entitled *Urgent Upgrade; Protect Public Values in our Digitized Society* (Kool, Timmer, Royakkers, & Est van, 2017). Based on a comprehensive literature review (Royakkers, Timmer, Kool, & van Est, 2018), Rathenau elicited seven urgent and recurring themes of ethical and social concerns. These themes are privacy, autonomy, security, controlling technology, human dignity, equity and inequality, and power relations (Kool, Timmer, Royakkers, & Est van, 2017, pp. 46-48; 71-74). The authors recognize that these themes manifest themselves differently, depending on the technological area under study. Like environmental pollution, data pollution, as illustrated in their literature review, also appears in many forms and disguises.

Other frameworks for classifying harms caused by data pollution have been considered, such as the Capabilities Approach, Human Rights, Well-being, Human Agency and Responsible Research and Innovation. The OECD has applied its well-being framework to the digital transformation (OECD, 2019, p. 22), and most of its dimensions of opportunities and risks can be matched with the Rathenau themes.

In their pape*r From Footprint to MindPrint*, Gertsen and Oosterlaken (2018, p. 28) argue that corporations have an incentive to disclose responsible innovation processes and the related positive contributions to consumer well-being. Based on research carried out by Rathenau and also following earlier work by Gertsen and Oosterlaken (2018), we believe that five (out of seven) Rathenau themes provide a practical framework to assess harms caused by data pollution, as follows:

- Privacy: including protecting personally identifiable information, safeguarding mental and spatial privacy, protection against surveillance
- Autonomy: freedom of choice, freedom of expression, manipulation, paternalism (Susser, Roessler, & Nissenbaum, 2019)
- Safety and Security: information security, no identity fraud, physical safety (Solove & Citron, 2017)
- Human dignity: dehumanization, instrumentalization, deskilling, desocialization, unemployment (Floridi, 2016)
- Equity and equality: discrimination, exclusion, unequal treatment, unfair bias, stigmatization

[15] Rathenau Instituut was founded in 1986 by the Dutch Government. It conducts independent research on the impact of technology on human lives and society, see https://www.rathenau.nl/en/about-us/who-we-are

The harm dimensions, elicited from the Rathenau research, consist of five separate harms that, in our view, and based on the extensive literature study in Chapter 2, provide appropriate measures of damages caused by data pollution.

3.4 Taxation of Negative Externalities - Overview

The origin of defining negative externalities and their possible taxation remedies can be found in *The Economics of Welfare*, published in the 1920 first edition by Pigou (2013). The author states 'Yet again, third parties - this time the public in general - suffer incidental uncharged disservices from resources invested in…' (Pigou, 2013, p. 186); and continuous a few pages after that: 'The most obvious forms which these encouragements and restraints may assume are, of course, those of bounties and taxes' (Pigou, 2013, p. 192). Following Pigou, taxation as a policy instrument to control negative externalities has been accepted and is well established in economics (Baumol, 1972; Diamond & Mirrlees, 1971; Edenhofer, Franks, & Kalkuhl, 2021).

More recently, taxing negative externalities caused by environmental pollution has also been well covered in taxation literature (Carattini, Kallbekken, & Orlov, 2019; Connolly, 2015; Daniel et al., 2017). Moreover, suppose environmental pollution taxes can be used to decrease other distortionary taxes (for example: tax base erosion and profit shifting), and at the same time improve environmental quality. In that case, the pollution taxes will lead to what Goulder (1995) calls a double dividend.

Currently, there is considerable debate, both in public and in academia, on how and where profits made by digital platforms should be taxed, see Köthenbürger (2020); Sanchez-Cartas (2020). However, this thesis addresses the taxation of data sharing only from a data pollution perspective. A solution proposed by Ben-Shahar (2019, p. 142) is a data tax. This tax is to be levied both on the data giver and on the data harvester and processor. In his view, this data tax on the data sharer would make individuals more aware of data pollution and lead to fewer 'data discounts', defined as paying with data to get platform service. Thus, taxation could curb harms caused by unbounded and costless data sharing.

In considering what would be an appropriate tax rate, we have used absolute levels of taxation in the individual pollution cases and an incremental tax rate (so a percentage on top of regular corporate tax rates imposed) applicable to corporate data pollution, rather than average or progressive rates. A significant reason for this is simplicity in concept and to avoid respondents applying prejudice based on their local (state) tax situation. For individual cases, the tax would be collected through the monthly internet charges - ranging from zero to forty US Dollars. The extra tax on top of ordinary corporate profit tax was set in a percentage range of zero to a maximum of fifty per cent.

The purpose of taxing data pollution is to internalize the cost or damages of externalities associated with data pollution. In line with discussion on the design of a carbon pollution tax (Metcalf & Weisbach, 2009), collecting the data pollution tax up-stream has the advantage that at the level of significant data controllers (the large social media platforms and data brokers), the number of substantive taxpayers shall be limited. Therefore, any tax collection issues envisaged would be considered by respondents to be minimal.

To our knowledge, this is a first attempt to assess whether a data pollution tax is considered appropriate by individual data subjects. Due to the limited scope of this thesis, no inquiry will be conducted under corporate data controllers to assess whether they deem a data pollution tax appropriate for harms caused by their data pollution.

3.5 Data Pollution Taxation and Anticipated Changes in Data Sharing Behaviour

Will taxation of data pollution change the behaviour of actors that cause data pollution? Governments can use taxation to regulate individual, collective, and corporate behaviour (Guler, 2019). Next, as discussed before, taxation is also used as a mechanism to control negative externalities when these externalities cause pollution to the environment (Baumol, 1972; Carattini et al., 2019; Connolly, 2015; Edenhofer et al., 2021). Recent interest in developing data pollution taxation has been stimulated by Romer (2021) and Ben-Shahar (2019, pp. 138-143). Finally, and comparable to pollution taxes, so-called 'sin taxes' are an instrument that governments use to limit or ban unhealthy behaviour (Braillon, 2012; Gruber & Koszegi, 2002; Lorenzi, 2004; O'Donoghue & Rabin, 2006).

As taxation will increase the price of products and services, we expect that imposing a tax on individual data sharing practices and taxation of corporate data extraction will decrease data transmissions that are qualified as data pollution. Based on the considerations of the previous two paragraphs on the effects of taxation on behaviour, we believe that next to testing the total direct relationship between data pollution harms and the anticipated change in behaviour, taxation will play a mediating role in establishing that relationship. Hence the hypothesis **H1** through **H4** will also be tested using mediation analysis. These considerations of data pollution harms lead us to construct an essential part of the following hypothesis. We believe that the higher the damages are caused by data pollution, the higher individuals will rate their anticipated change of data sharing behaviour, as follows (for individual data pollution instances):

> ***H1**. If persons rate the perceived overall harm (as the average of five individual harms) caused by individual data pollution higher, then they believe that the nominal data pollution tax to be levied on individuals should be higher, and accordingly, the change (decrease) in data sharing behaviour to be more significant.*

And, similarly for corporate data pollution instances:

> ***H2.** If persons rate the perceived overall harm (as the average of five individual harms) caused by corporate data pollution higher, then they believe that the incremental data pollution tax to be levied on corporations should be higher, and accordingly, the change (decrease) in data sharing behaviour to be larger.*

3.6 Intent to Share Data

The literature review supporting the development of the various data pollution cases shows that technological affordances play a very dominant role in the data sharing behaviour of individuals. These affordances act as commercial catalysts of data sharing behaviour (Zhou & Rau, 2021). They are also designed to entice others to participate in contagious behaviour (Guadagno, Rempala, Murphy, & Okdie, 2013). Affordances aim to provide users of data sharing applications with increasingly clear information to act on. At the same time, the affordance’ design maximizes intent to utilize the data sharing capabilities provided by the application for the user (Conole & Dyke, 2004). However, these seemingly positive attributes of affordances often lead to addiction and contagion effects of social media usage (A. Chen, 2019). Moreover, these affordances can lead to moral contagion in these networks (Burton, Cruz, & Hahn, 2021). Suppose affordances play such an essential role in data sharing behaviours. In that case they will also contribute to the sharing of data of others and thereby play a crucial part in cascading data pollution and its harms.

The table below provides an overview of how the various vignettes can be grouped in four quadrants to summarize and assess the combination of harms and sharing intent. By including questions in the survey on both the overall severity of harm and perceived intent of sharing, we will be able to categorize pollution vignettes.

Intent High	High Intent to share - Low Harm	High Intent to share - High Harm
Intent Low	Low Intent to share - Low Harm	Low Intent to share - High Harm
	Harm Low	**Harm High**

The review of the literature in Chapter 2 on technological affordances that enable data pollution and our related expectations regarding the contagious effects of these affordances lead us to draw up the following hypotheses:

> ***H3.*** *If persons rate the intent of spreading data by individuals to be higher, then they believe that the nominal tax rate to be levied on individuals should be higher, and accordingly, the change (decrease) in data sharing behaviour to be larger.*

And, similarly for corporate vignettes:

> ***H4.*** *If persons rate the intent of spreading data by corporate polluters higher, then they believe that the incremental data pollution tax to be levied on corporations should be higher, and accordingly, the change (decrease) in data sharing behaviour to be larger.*

As an academic topic of interest, data pollution has only recently been developed. In the previous paragraphs, we explained that we will use short case studies (vignettes) to elicit the respondents' views on potential harms caused by data pollution and whether data sharing behaviour should be taxed to limit data sharing behaviour and its damages. To gauge whether respondents have an adequate understanding of the data pollution concept after having read the various pollution case studies, we will test the following hypothesis:

> ***H5.*** *Individuals at the end of the survey (after having absorbed the data pollution vignettes) will rate the necessity for a data pollution tax higher, compared to their views thereon at the beginning of the survey.*

3.7 Data Pollution Behavioural Changes: Comparing Self and Vignette Actors

Individuals tend to admit socially desirable behaviour and deny socially undesirable traits. Put differently, respondents in survey research tend to attribute to themselves statements which are socially desirable and reject statements that are considered socially undesirable (Chung & Monroe, 2003; Fisher, 1993; Furnham, 1986). Indirect questioning, such as responding to an actor's behaviour in case studies (vignettes), also called the third-person effect, results in a reduction of social desirability bias of respondents (Fisher, 1993; Perloff, 1999). Next to the social desirability bias, the 'better than average' effect is also expected to play a role in respondents answering questions on their own behavioural change (Alicke & Govorun, 2005; Zell, Strickhouser, Sedikides, & Alicke, 2020). However, due to the limited objective of this thesis, we will not endeavour to analyse the differences between respondents own behavioural change anticipation and the perceived change in vignette actor's behaviour.

For these reasons, the survey utilises two question formats on expected behavioural change. First, we will ask the respondent to indicate behavioural change caused by data taxation of the vignette actor. Thereafter, we will ask the respondent about his own behavioural change if data sharing behaviour would be taxed. Based on these considerations we have formulated the following hypotheses:

> ***H6.*** *If individuals would be taxed on data pollution, they will limit their own data pollution behaviour to a larger extent compared to the vignette actors.*

And, similarly for corporate data pollution vignettes:

> ***H7.*** *If individuals would be the CEO of the corporation to be taxed for data pollution, they would limit the data pollution activities of the corporation to a larger extent compared to that of the vignette corporation.*

3.8 Additional Testing of the Overall Harm Construct

Recent scandals of Covid misinformation, massive data breaches, Cambridge Analytica, and the Facebook revelations by a whistle-blower in 2021 have created, in our view, sufficient public awareness as to what these harm dimensions entail. Based on that public awareness, we believe it is adequate to directly ask our survey respondents about their assessment of these harm dimensions when confronted with a data pollution case study (the vignettes). The dimensions 'Control over Technology' and 'Balance of Power' of the Rathenau research are of more relevance in studying the relationship between actors. For that reason, they are excluded from the list of harms in this research. However, to ensure that the five harm dimensions that we have used to test H1 and H2, we will also test the adequacy of these five harms as representing key dimensions of harms to human well-being. For that reason, we have developed the following hypotheses:

> ***H8a. (Individual Vignettes)*** *If persons rate harm to privacy, autonomy, dignity, security, and equality higher, then the perceived overall harm caused by data pollution is rated higher.*
>
> ***H8b. (Corporate Vignettes)*** *If persons rate harm to privacy, autonomy, dignity, security, and equality higher, then the perceived overall harm caused by data pollution is rated higher.*

3.9 Elasticity of internet Services and Data Sharing.

The average price of broadband internet access in the US is around $ 60[16]. Demand elasticity of

[16] How much is internet? See: https://www.reviews.org/internet-service/how-much-is-internet/ and https://www.highspeedinternet.com/resources/how-much-should-i-be-paying-for-high-speed-internet-resource

internet service is estimated by Wilson (2017) to be moderately inelastic (between - 0.5 and - 0.6). This implies that internet services in general are viewed as an essential service. Consumers believe they need internet connection as a basic good and therefore a certain percentage of price change would not lead to a similar level of change in demand. For example, and based on the elasticity mentioned, the decrease in demand would be limited to half of the price increase.

However, if a good or service has many close substitutes, as is the case with internet usage and social media applications, the demand for such services is expected to be highly elastic within that group. Substitutes for data transmissions using the internet, can also provide many positive, perhaps less-polluting alternatives. 'Any one of a group related products or services will tend to have an elastic demand, even though the demand for the group (in this case broadband data transmissions) as a whole may be inelastic (Chrystal & Lipsey, 1997, p. 95). On that basis, consumers will switch from a higher priced service to a lower priced if the cheaper service can act as a substitute and has approximately the same utility to the user.

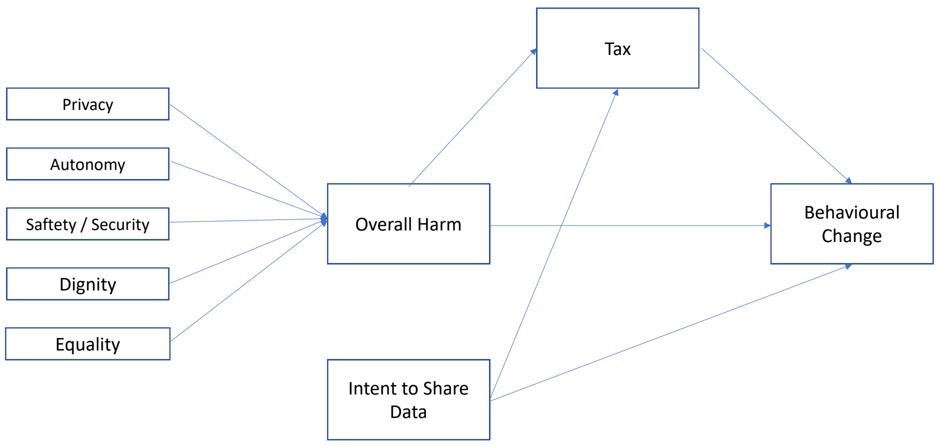
The variable *elasticity* will be computed and reflects the relative adaptation of *data sharing behaviour change to data sharing tax.* In other words, elasticity is computed by dividing the movement in *data sharing behaviour change* by the additional *data sharing* tax to be levied. The concept of elasticity is used in economics to determine whether demand, in our case for data sharing applications (and social media usage), is sensitive to price increase, in this research caused by a pollution tax. We decided to calculate the *elasticity* to determine how the various instances of data pollution (the vignettes) can be ranked in order of relative price sensitivity. When goods or services within a group incur price increases, the demand for those goods will shift to those with a smaller, or no, price increase (Chrystal & Lipsey, 1997, pp. 95 - 96). Based on the above considerations the following hypotheses have been developed:

> ***H9.*** *The higher the overall harm, a higher elasticity of demand is expected (a higher change in data sharing behaviour in our case).*
>
> ***H10.*** *The higher the intent to spreading, a higher elasticity of demand is expected (a higher change in data sharing behaviour in our case).*

3.10 Basic Research Model

Following from our literature review on data pollution and its instances, in this chapter, we have now formulated several hypotheses on the expected relationships between data pollution harms and changes in data sharing behaviour if a data pollution tax would be levied. Next to overall harm, we also believe that 'Intent to Share' will play a role in the behavioural change of data pollution activities. The Research Model can be illustrated by the graphical illustration depicted below. In the next paragraph, we will present a short overview of the mediation model we plan to use to analyse our hypotheses **H1** through **H4**. The other hypotheses (**H5** through **H8**) will be tested using various t-tests and multiple linear regression analyses to investigate our claims from **H5** through **H8** and will be explained in more detail in the Methods section.

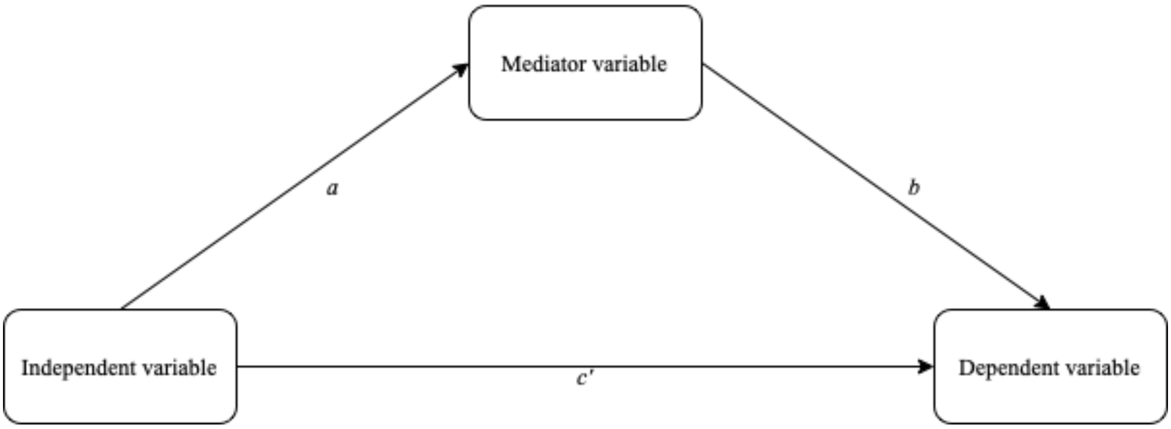
Graphical Illustration of Data Pollution and Taxation Model



3.11 Mediation Analysis Model

We suspect that taxation will influence the causal relationship between harms caused and behaviour change. We therefore choose to use mediation analysis. Mediation analysis is used to gain a deeper understanding of how variables are related. In other words, it is an exercise to understand the underlying causal mechanisms (Hayes, 2018) between certain variables and variable(s) that mediate those relationships. The most basic mediation model is the simple mediation model displayed in Model 1. In the simple mediation model, the dependent variable has two causal antecedents, the mediator variable, and the independent variable. Moreover, the independent variable also is the antecedent of the mediator variable. Hence, the mediator variable is an antecedent and a

Model 1. Simple mediation model.



consequent in the same model.

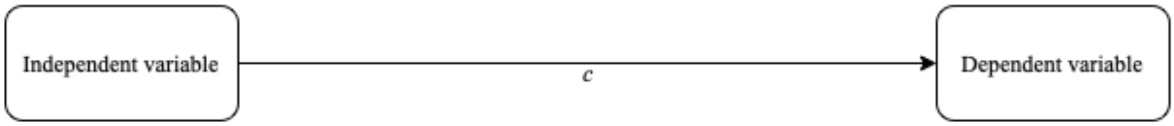
In the mediation model, the relation between the independent and dependent variables, displayed by the pathway c′, is considered the direct effect. The direct effect can be interpreted as a one-unit change in the independent variable, leading to a change of c′ units on the dependent variable while holding the mediator variable constant. In other words, the direct effect is the difference in the dependent variable for two respondents with identical scores on the mediator variable.

The so-called indirect effect of the independent variable on the dependent variable is through the mediator variable, hence taking pathways a and b together, or ab. The indirect effect is the product of the two separate effects, a and b. It can be interpreted as: a one-unit change on the independent variable is predicted to change the dependent variable by ab units. There are two ways to infer the statistical significance of an indirect effect, according to Hayes (2018, pp. 82 - 85). The first way, the normal theory approach, calculates a standard error term based on the two standard error terms of a and b and consequently delivers a common p-value. Yet, it relies on the assumption that the sampling distribution of the indirect effect is normal, which usually is not given. A more robust method uses a 95% bootstrap confidence interval of the estimated coefficient, which does not make any assumption about the sampling distribution (Hayes, 2018, pp. 97 - 98). Therefore, we chose to use the bootstrapping method for 5,000 bootstrapped samples. The bootstrapping process ultimately gives one a confidence interval, and for the indirect effect to be considered significant, the two values of the interval have to be either both positive, or both negative. Otherwise, the indirect effect cannot be viewed as substantial.

In this thesis, we use mediation analysis described by Hayes (2018), and we do not previously establish if the relationship between the independent and dependent variable is significant. Instead, we aim to understand the indirect effect. Nonetheless, to give a comprehensive summary of mediation analysis, we will address the so-called total effect hereafter[17].

The total effect is the effect of the independent variable on the dependent variable when we ignore the presence of the mediator variable. In other words, a one-unit change on the independent variable leads to a c unit change on the dependent variable. Model 2 illustrates this relation where c is the total effect. Importantly, when using Ordinary Least Squares (OLS), regression c can be perfectly partitioned into ab + c'. Thus, adding the indirect and direct effect together results in the total effect of the independent variable on the dependent variable. However, the understanding and interpretation of the total effect are only of secondary nature to this study, and

Model 2. Total effect.

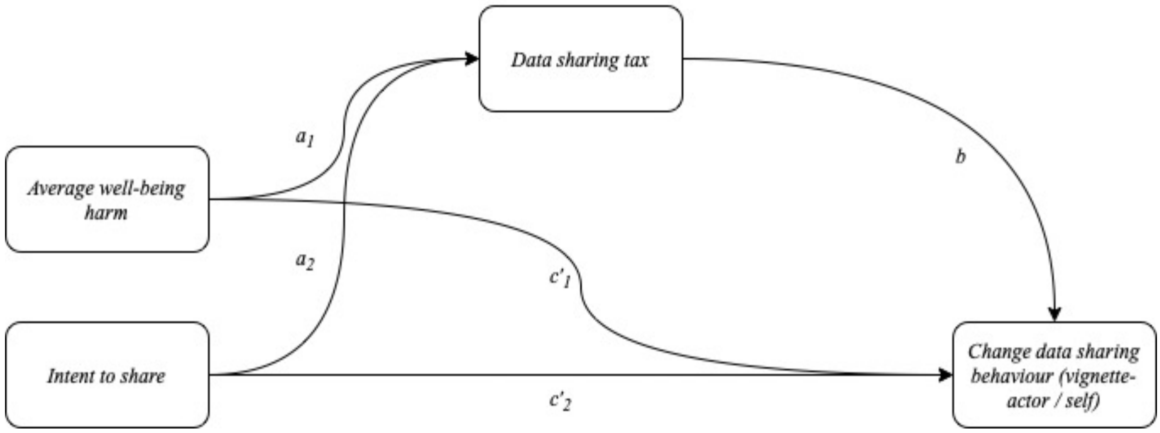


we focus on the direct and indirect effects

As discussed previously in this study, we aim to deepen our understanding of how the perception of harm to the well-being of a nonparticipant through data pollution can effectively be limited. We suggested that imposing an additional tax on data pollution would correct such undesirable externalities by curbing data pollution behaviour. In this scenario, the perception of harm to the well-being of a nonparticipant would lead to an additional data pollution tax which would, in turn, lead to an adjustment in behaviour that is potentially identifies as data pollution (**H1** and **H2**). Analogous to the harms to the well-being of a nonparticipant, we argued for the effect of the intent to share to change data pollution behaviour through levying and additional tax (**H3** and **H4**). Accordingly, we have two independent variables which is slightly different from Model 1. Model 3 gives a visualisation of the hypothesised mechanisms. This also means we have two distinct indirect and direct effects of intent to share and well-being harms.

[17] For a more detailed overview of mediation analysis, including a discussion of the total effect please refer to (Hayes, 2018, pp. 82 - 85). *Introduction to Mediation, Moderation, and Conditional Process Analysis* (2nd edition).

Model 3. Hypothesised mediation model.



3.12 Overview of Hypotheses

H1. *If persons rate the perceived overall harm (as the average of five individual harms) caused by individual data pollution higher, then they believe that the nominal data pollution tax to be levied on individuals should be higher, and accordingly, the change (decrease) in data sharing behaviour to be more significant.*

H2. *If persons rate the perceived overall harm (as the average of five individual harms) caused by corporate data pollution higher, then they believe that the incremental data pollution tax to be levied on corporations should be higher, and accordingly, the change (decrease) in data sharing behaviour to be larger.*

H3. *If persons rate the intent of spreading data by individuals to be higher, then they believe that the nominal tax rate to be levied on individuals should be higher, and accordingly, the change (decrease) in data sharing behaviour to be larger.*

H4. *If persons rate the intent of spreading data by corporate polluters higher, then they believe that the incremental data pollution tax to be levied on corporations should be higher, and accordingly, the change (decrease) in data sharing behaviour to be larger.*

H5. *Individuals at the end of the survey (after having absorbed the data pollution vignettes) will rate the necessity for a data pollution tax higher, compared to their views thereon at the beginning of the survey.*

H6. *If individuals would be taxed on data pollution, they will limit their own data pollution behaviour to a larger extent compared to the vignette actors.*

H7. *If individuals would be the CEO of the corporation to be taxed for data pollution, they would limit the data pollution activities of the corporation to a larger extent compared to that of the vignette corporation.*

H8a. (Individual Vignettes) *If persons rate harm to privacy, autonomy, dignity, security, and equality higher, then the perceived overall harm caused by data pollution is rated higher.*

H8b. (Corporate Vignettes) *If persons rate harm to privacy, autonomy, dignity, security, and equality higher, then the perceived overall harm caused by data pollution is rated higher.*

H9. *The higher the overall harm, a higher elasticity of demand is expected (a higher change in data sharing behaviour in our case).*

H10. *The higher the intent to spreading, a higher elasticity of demand is expected (a higher change in data sharing behaviour in our case).*

4 Methods

4.1 Participants and Procedures

The survey respondents were recruited by way of CloudResearch and by engaging Amazon Mechanical Turk workers (MTurk), for details see Litman and Robinson (2020). CloudResearch is a research management system specifically developed for MTurk to facilitate the data collection through MTurk for researchers. Furthermore, MTurk is a for-pay online service where survey requesters can post so-called Human Intelligence Tasks (HITs), such as surveys, which get completed by MTurk's online workforce. MTurk has about 250,000 workers worldwide, with most workers coming from the US (Robinson, Rosenzweig, Moss, & Litman, 2019).

Sampling respondents for academic surveys using MTurk has shown similar reliability as traditional recruitment methods (Mason & Suri, 2012, p. 3; Paolacci, Chandler, & Ipeirotis, 2010, pp. 414 - 415). Furthermore, CloudResearch provides tools that enable survey sampling across different times of the day and throughout days of the week, thereby preventing various potential sampling biases (Arechar, Kraft-Todd, & Rand, 2017; Fordsham et al., 2019). MTurk can also include or exclude workers based on MTurk worker level, level of schooling, household income, investment experience, social media experience, and several other demographical criteria. Workers of 'any level' were selected and for those workers a HIT Approval Rate >90% was required. These participants also needed to have completed a number of approved HITs in excess of 1,000 (Litman & Robinson, 2020, pp. 64 - 65). The survey questions on levels of taxation were tailored to the US environment and for that reason, location of workers in the sample was limited to the United States. To obtain a sample representative of the US population, no other demographic selection criteria were used. Workers who accepted to complete the survey were provided with a 'secret code' that confirms to both Qualtrics (an online survey tool) and CloudResearch that the respondent has completed all questions of the survey before submitting the HIT.

The survey was developed in Qualtrics (Qualtrix, 2020). It contained various demographic questions, questions about opinions of the respondent and 18 different vignette stories. The vignettes were divided over distinct categories. The first category consisted of nine individual-actor vignette stories and the second category equally consisted of nine corporate-actor vignette stories. The vignettes from both categories were matched. For instance, one individual-actor vignette presents a story about Julia's use of the fitness app Strava and how her data sharing behaviour causes negative externalities for nonparticipants, the matched corporate-actor vignette presents a story about how telecom providers share geo-location data with immigration authorities and how this non-consented data sharing crates negative externalities as well. A full overview of the vignettes can be found in Appendix X (Final Vignettes); Appendix Y for an overview of how Individual Vignettes are linked with Corporate Vignettes.

To reduce the length of the survey and consequently improve the obtained data quality we limited the number of vignettes assigned to each respondent (Deutskens, De Ruyter, Wetzels, & Oosterveld, 2004; Gross, Lorek, & Richter, 2017). We based the time estimate per vignette on a pilot study that was conducted with a selection of the current vignettes. Consequently, we decided that each respondent will be randomly assigned to either the individual vignettes or the corporate vignettes, thus each respondent would consider nine vignettes. For participants, the order of the vignettes was randomized by Qualtrics to avoid possible order effects (McFarland, 1981).

Before filling out the survey the respondent was informed about the purpose of the study, the research procedure, and the confidentiality measures to protect their data. Thereafter the participants were asked to give their consent to being subject in a research study, as well as asked to indicate that they participate out of their own free will. If the respondents would answer in the negative, then they could not participate in the study. Respondents that completed the survey were compensated through the MTurk’s application programming interface.

In total 622 respondents filled out the survey. 313 respondents completed the individual-actor vignettes and 309 filled out the corporate-actor vignettes. Roughly 52% of all participants identified as male and 47% as female, the remaining 1% consisted of participants that identified by a third gender or preferred not to indicate their gender. The average age of the participants was 41.5 years and ranging from 20 to 77 years of age.

4.2 Measurements

Based on our basic research model (previous chapter, par 3.9), the following measurements have been developed.

Data pollution tax effectiveness. The variable *data pollution tax effectiveness* consisted of one item and was measured twice. Once before any vignette was introduced and once at the end of the survey, when respondents had been able to absorb the data pollution examples by responding on the vignettes. The item stated ’Currently, I believe that levying a tax on harmful data sharing and data extraction practices will decrease data transmissions.’. The item was measured on a 5-point Likert scale ranging from (1) *strongly disagree* to (5) *strongly agree*.

Well-being dimensions. The perceived effects of data sharing practices on well-being of a nonparticipant (the subject(s) in the vignette, potentially harmed by the vignette actor) were measured by five items. Each item represented one dimension of possible negative effects on well-being, namely *Privacy, Autonomy, Safety and Security, Human Dignity* and *Equality* (Kool, Timmer, Royakkers, & Est van, 2017). The respondents were asked about the extent to which action(s) described in the vignette had a negative influence on the well-being dimensions of the nonparticipants). For the dimension of *Privacy,* the item stated, ‘Privacy of <Nonparticipant> is impaired’, for *Autonomy* it stated, ‘Autonomy of <Nonparticipant> is diminished’, for *Safety and Security* the item read ‘Safety and security of <Nonparticipant> is put at risk’, for *Human dignity* it stated, ‘Human dignity of <Nonparticipant> is harmed’ and for the dimension *Equality* the item read, ‘Equality of <Nonparticipant> is damaged’. The items were measured on a 5-point Likert scale ranging from (1) *Strongly disagree* to (5) *Strongly agree*.

Overall well-being harm. The variable *overall well-being harm* was measured by asking the respondent to indicate the overall harm severity inflicted by the vignette actor on the nonparticipant of the described data sharing behaviour. The item was measured on a 5-point Likert scale ranging from (1) *Not severe, no harms* to (5) *Very significant harms*.

Intent to share. The measurement for the variable *intent to share* stated ‘Intent of <Actor> to share data with <Third Party>’. The respondent could answer on a 5-point Likert scale ranging from (1) *No intention to share at all* to (5) *Full intention to share with as many others as possible*.

Data sharing tax. The variable *data sharing tax* was measured in two distinct ways depending on whether the respondent was reacting to an individual-actor or a corporate-actor vignette. The item for the individual-actor vignette stated ‘If a personal data sharing tax is levied, I believe that <Actor> data sharing should be taxed as follows’. The respondent was asked to indicate their answer from 0$ to 40$ by using a slider which indicated *Additional Dollar’s tax on <Actor> monthly internet bill*. For the corporate-actor vignettes the item stated ‘If an additional corporate data sharing tax is levied, I believe that <Actor> should be taxed as follows’. The respondent was asked to indicate their answer from 0% to 50% additional tax on data sharing profits of <Actor> by using a slider which indicated *Additional percentage (%) tax on <Actor> data sharing profits*.

Data sharing behaviour change. The variable *data sharing behaviour change* was measured in two different ways depending on whether the respondent was reacting to an individual-actor or a corporate-actor vignette. Moreover, two items were used to measure the variable. For both vignette categories the question once concerned the actor introduced in the story and once it concerned the respondent directly. The decision to use two items relates to the social desirability bias in answers to questions about oneself (Chung & Monroe, 2003; Fisher, 1993). Generally, participants like to present themselves in a more favourable light which could cause them to show greater adjustment of undesirable behaviour. The items for the individual-actor vignettes stated, ‘If taxed, I believe that <Actor> will decrease their data sharing to the following extent’ and ‘If I would share data as did <Actor> and it would be taxed, I would decrease my data sharing as follows’. The answer options ranged from 0% to 100% with 1% increments. For corporate-actor vignettes the items stated 'If taxed, I believe that <Actor> will decrease its data sharing practices with the <Third Party> as follows' and 'If I would be the CEO of <Actor>, and sharing of <Nonparticipant> data would be taxed, I would decrease data sharing as follows'. Again, the answer options ranged from 0% to 100% with 1 percentage points increments.

Covariates. Various demographic variables were collected. Respondents were asked to indicate their *Gender* by selecting one of four categories (1) *Male*, (2) *Female*, (3) *Non-binary / Third gender* and (4) *Prefer not to say.* The respondent was asked for their *Age.* Furthermore, they were asked about their *Race / Ethnicity* with the following categories (1) *European American / White*, (2) *African America / Black*, (3) *Hispanic / Latino*, (4) *Asian*, (5) *Other*. Next, the respondents were asked to indicate their educational level with the following answer categories (1) *Eighth Grade or less*, (2) *High school degree*, (3) *Some college*, (4) *Bachelor's degree*, (5) *Master's degree*, (6) *Professional degree (JD, MD, MBA)* or (7) *Doctoral degree (PhD)*. Lastly, the respondents were asked about their *political party preference* with the answering options (1) *Republican*, (2) *Democrat*, (3) *Other*, (4) *Prefer not to say*.

4.3 Analysis

The various analyses were performed in the statistical software SPSS (version 27.0, IBM Statistics, 2020). To analyse the proposed mediation model, we used the so-called PROCESS macro from Hayes (2018). All regression models were estimated using Ordinary Least Squares (OLS) which minimises the sum of squared residuals for the model. No cases with missing data had to be excluded from the analyses. However, if a participant indicated that 0% additional tax should be levied, we had to exclude this case[18] from the mediation analysis and regression analysis. The reason is that there is an internal disconnect between the then levied tax of 0% and the resulting behavioural change as a reaction to the tax. The disconnect results from the phrasing of the question for the variable *data sharing behaviour* which assumes an additional levied tax. Consequently, we cannot assume a causal link between these variables anymore, and causality is a requirement for mediation and linear regression analysis (Hayes, 2018). In total, 27 participants had to be excluded from these analyses, since they indicated 9 out of 9 times for their respective vignettes that the additional levied tax should be 0. The 27 were distributed into 20 participants of the individual vignettes and 7 of the corporate vignettes.

[18] Notably, case here does not refer to the respondent, but just to the respective answers to the measurements of *data sharing behaviour* and *data sharing tax* of the respective vignette.

The analysis was divided into three sections. First, we performed various analyses on the so-called overall models, these are the models where we averaged all vignette scores for the two types of vignettes. In other words, each variable, such as *intent to share*, had its average calculated from all nine scores of the respective vignette type. We inspected the correlations of these variables, as well as their means, standard deviations and whether they follow a roughly normal distribution. For the assessment of the normal distribution, we will calculate the z-score of skewness and kurtosis which should not exceed 3.29 (Kim, 2018)[19]. For the normality of the distribution, we focus on the dependent variables. In essence, the assumption of normality states that the residuals of the predicted values follow a normal distribution, and hence, are most strongly related to the dependent variables (Hayes, 2018). Therefore, we will inspect the indicators of normality for the variables *data sharing tax, data sharing behaviour change (self)* and *data sharing behaviour change (vignette-actor)*. We tested the normality of the distribution of the dependent variables.

Additionally, we inspected whether the respondents' demographics lead to some striking differences in scores. After these more descriptive steps we performed the mediation analysis and ran the multiple linear regression analysis to test our hypotheses for the two overall models. We tested H1, our expectation that the positive relation between *overall data sharing harm* and *data sharing behaviour* is mediated by the levied *data sharing tax* by using the mediation model as discussed by Hayes (2018). Analogously, we tested our expectation that the positive relation between *intent to share* and *data sharing behaviour* is mediated by the levied *data sharing tax* (**H3**). Notably, we had to run the whole mediation analysis twice for each model, since the modelling procedure is limited to only calculating the *indirect effect* for one independent variable at a time. Thus, one of our independent variables was specified as the independent variable in the model and the other was added as a simple covariate. The multiple linear regression analysis tested our hypotheses **H9** and **H10**, hence our expectations that greater *well-being harms* and greater *intent to share* will increase the *elasticity of behaviour* for each type of vignette.

Second, and to gain deeper insight into the different types of data pollution we made smaller categories for the two types of vignettes by means of exploratory factor analysis (EFA). We investigated whether we could find patterns in the well-being harm dimensions between the various vignettes. It would not be surprising if the various vignettes shared specific characteristics in the way they affect the well-being of the nonparticipant. For instance, some vignettes may be deemed to harm the privacy of the nonparticipant, while others are more severely damaging to human dignity. Through the EFA we hope to detect specific shared patterns between vignettes which would allow us to group them together. Moreover, the additional created detail through the categorisation may

[19] The z-score can be calculated by dividing the respective score of skewness or kurtosis by its standard error.

help get deeper insights into if well-being harm clusters. Grouping of vignettes might also reveal how differences in data pollution affect the effectiveness of a tax intervention to limit such behaviour.

We structured our EFA according to the article by Osborne and Costello (2005). Therefore, we used maximum likelihood estimation as our factor extraction method. Additionally, we picked orthogonal rotation, and eigenvalue greater than 1[20] and only considered items to be part of a rotated factor if their *item loading* was higher than .3 and not cross-loading[21]. From the suggested solutions we matched those vignettes which related most often and distinctively to the same factors. Notably, we calculated new averages for each of the variables based on their new assigned vignette category. Thereafter, we repeated the hypotheses testing from the overall model for the newly created vignette categories.

Third, we performed various t-tests and another multiple linear regression analyses to investigate our claims from **H5** through **H8**. For these analyses we were able to use the full samples again and could ignore the fact that some respondents indicated (for all nine vignettes) that the additional data tax to be levied should be zero. Moreover, we generally used the averages from all vignettes for each variable. The expectation that the respondents would rate the necessity for a data pollution tax higher at the end of the survey (after having absorbed the data pollution vignettes) compared to their views at the beginning of the survey (**H5**), was tested using a one-sample t-test. The hypothesis that individuals would change their own behaviour to a greater extent than the behaviour of the vignette-actor for the individual vignettes (**H6**) was also tested with a one-sample t-test. The analogous hypothesis for the corporate vignettes (**H7**) was tested using a one-sample t-test. Lastly, the hypothesis that all well-being harm dimensions show a positive relation with the reported overall harm for the individual vignettes (**H8a**) and the corporate vignettes (**H8b**) was tested using multiple linear regression.

[20] We are aware that using the eigenvalue greater than one rule may lead to overestimation of extracted factors and that we must exercise some caution in their interpretation.
[21] We consider cross-loading to be the case if an item has more than one item loading greater than .3.

5 Results

5.1 Overall Model

In the overall model, we differentiate our investigation into two vignette classes. Vignettes grouped into the 'individual' class and vignettes belonging to the 'corporate' class. In Table 1, we can see that the specific well-being harms and the *overall well-being harm* for the individual-type vignettes all seem to be above the mid-point of their scales[22]. The same appears to be true for all the measurements apart from *data sharing behaviour change* (vignette-actor), where the average falls almost precisely on the scale's mid-point[23]. For the corporate-type vignettes, as seen in Table 2, we can see a very similar pattern for all the individual well-being harms and the *overall well-being harm*, *intent to share* and the *data sharing tax*; all of these variables seem to have means that are above the mid-point of their scales. However, for the corporate-type vignettes, the mean of *data sharing behaviour change (self)* is only slightly above the scale's mid-point. For *data sharing behaviour change (vignette-actor)*, it is clearly underneath the mid-point of its scale.

We tested the normality of dependent variables. For the individual-type vignettes, the standardised skewness for *data sharing tax* (z-skewness = -3.394) and *data sharing behaviour change (self)* (z-skewness = -9.676) exceed the critical value of 3.29. Moreover, standardised kurtosis of *data sharing behaviour change (self)* (z-kurtosis = 5.014) also exceeds the critical value. Accordingly, the assumption of normality of residuals is violated. For the corporate-type vignettes, only the standardised skewness value of *data sharing behaviour change (vignette-actor)* (z-skewness = 3.342) exceeds the critical value, and all standardised kurtosis values are below 3.29. Despite the violation of the normality assumption, we will continue with the variables as given now. OLS estimation is relatively robust against violation of the normality assumption (Hayes, 2018). Moreover, changing values by using arithmetic can complicate the interpretability of the results (Pek, Wong & Wong, 2018).

Next, we performed various analyses of variance (ANOVAs) to see whether some of our variables show differences based on the respondents' *political orientation* and *gender*. For the individual-type vignettes, 96 respondents indicated to have voted republican in the last election, 180 had voted democrats, 25 other and 12 preferred not to say[24]. For the corporate-type vignettes, the distribution was quite similar; 84 respondents had voted republican, 180 democrats, 25 other and 14

[22] All these measurements were measured on a 5-point Likert scale; thus, the mid-point of the scale is 3.
[23] Here the mid-point of the scale is 50.
[24] For this analysis we used all participants because this analysis is not related to the mediation analysis and does not require causality between the variables.

preferred not to say. Since the sample size of the category 'preferred not to say' is very small and therefore hardly representative, we will not interpret the differences in means for this category. For the individual-type vignettes the one-way ANOVA revealed significant differences for all variables from the mediation model, hence *overall well-being harm* ($F(3, 309) = 9.841$, $p < .001$), *intent to share* ($F(3, 309) = 4.163$, $p = .007$), data sharing tax ($F(3, 309) = 5.709$, $p < .001$) and data sharing behaviour change (self) ($F(3, 309) = 3.596$, $p = .014$) and *data sharing behaviour change (vignette-actor)* ($F(3, 309) = 3.877$, $p = .010$). Additionally, the Tukey post-hoc test with Bonferroni corrected alpha levels of .0125 showed that respondents who voted democrats, scored significantly higher than the republican voters on variables *overall well-being harm* and *data sharing tax*. Additionally, democrat voters also scored higher than other voters for all variables. For the corporate-type vignettes, the only significant ANOVA for political orientation was on the variable *data sharing tax* ($F(3, 305) = 5.300$, $p < .001$). The results of the Tukey post-hoc test with Bonferroni correction (α = .0125) showed that democrat voters ($M = 31.106$, $SD = 10.605$) compared to the republican voters ($M = 26.392$, $SD = 12.291$) scored significantly higher.

For the variable *gender* we excluded the categories 'non-binary/third gender' and 'prefer not to say' from the ANOVAs, since their sample sizes did not exceed two and are therefore not representative. Accordingly, we ended up only comparing male and female respondents. Looking at the individual-type vignettes almost all variables the ANOVAs were significant, only *data sharing behaviour change (self)* ($F(1, 308) = 3.306$, $p = .070$) was not significantly different between men and women. For *overall well-being harm* ($F(1, 308) = 19.565$, $p < .001$) females ($M = 3.541$, $SD = 0.541$) scored higher than males ($M = 3.245$, $SD = 0.637$). For *intent to share* ($F(1, 308) = 11.556$, $p < .001$) females ($M = 3.640$, $SD = 0.434$) scored higher than males ($M = 3.466$, $SD = 0.468$) as well. Again, for *data sharing tax* ($F(1, 308) = 23.782$, $p < .001$) females ($M = 20.980$, $SD = 8.676$) also scored higher than males ($M = 16.118$, $SD = 8.877$). Lastly, also for *data sharing behaviour change (vignette-actor)* ($F(1, 308) = 4.405$, $p = .037$) females ($M = 47.562$, $SD = 18.895$) scored higher than males ($M = 43.097$, $SD = 18.554$). Looking at the corporate-type vignettes the results change and the differences between male and female respondents are only significant for *overall well-being harm* and *intent to share*. Females ($M = 3.896$, $SD = 0.590$) score higher than males ($M = 3.632$, $SD = 0.645$) for *overall well-being harm* ($F(1, 306) = 13.580$, $p < .001$), and also females ($M = 3.779$, $SD = 0.573$) score higher than males ($M = 3.587$, $SD = 0.535$) for *intent to share*.

Additionally, we ran a simple linear regression with *age* on the variables from the mediation model. For the individual-type vignettes *age* had a positive and significant effect on *overall well-being harm* ($b = .011$, $p < .001$), *intent to share* ($b = .008$, $p < .001$) and *data sharing tax* ($b = .110$, $p = .014$). In other words, for these three variables higher age predicts higher scores. For the corporate-type vignettes *age* had significant effects on *overall well-being harm* (b = .009, p = .002), *intent to share* (b = .008, p = .005), *data sharing behaviour change (self)* (b = -.265, p = .031) and *data sharing behaviour change (vignette-actor)* (b = -.343, p < .001). Hence, for *overall well-being harm* and *intent to share*, *age* has a positive effect, with increasing age these variables are scored higher. But, for the two measurements of *data sharing behaviour change* the effect of *age* is negative.

By looking at the correlations of the individual-type vignettes in Table 1 below, we can see that the variables generally appear to be related to how we expected them to be related. The *overall well-being harm* (r = .392, p < .001) and all specific harms, ranging from (r = .204, p < .001) to (r = .266, p < .001) positively and significantly correlate with *data sharing tax*. In other words, higher harms generally relate to a higher suggested data pollution tax. Moreover, *overall well-being harm* is positively associated with *data sharing behaviour change (vignette-actor)* (r = .187, p < .001) *while* not significantly correlated with *data sharing behaviour change (self).* Furthermore, none of the specific well-being harm dimensions shows significant correlations with either *data sharing behaviour change (vignette-actor)* or *data sharing behaviour change (self)*. *Intent to share* also indicates a significant and positive correlation with *data sharing tax* (r = .321, p < .001). Moreover, it shows a positive and significant relation with *change data sharing behaviour change (self*) (r = .177, p < .001), but *intent to share* does not indicate a significant correlation with *data sharing behaviour change (vignette-actor)*. Lastly, variable *data sharing tax* shows a positive and significant relation with *change data sharing behaviour change (self)* and with *change data sharing behaviour change (vignette-actor).*

For the corporate-type vignettes in Table 2 below, the correlations are like those of the individual-type vignettes. However, for the corporate-type vignettes, all the specific well-being harms, *overall well-being harm* (r = .256, p < .001) and *intent to share* (r = .177, p < .001) show significant and positive relations with *data sharing behaviour change (self).* And for *data sharing behaviour change (vignette-actor)*, the measures of human dignity, equality and equity, and *overall well-being harm* also show significant correlations.

Table 1. Mean, standard deviations and correlations for the averages of all individual vignettes (n = 293).

	Privacy	Autonomy	Safety and security	Human dignity	Equality and equity	Overall well-being harms (measured)	Average well-being harm (computed)	Intent to share	Data sharing tax	Data sharing behaviour change (self)	Data sharing behaviour change (vignette-actor)
Privacy		.761***	.707***	.717***	.675**	.685***	.845***	.290***	.228***	-.004	.100
Autonomy			.753***	.784***	.747***	.650***	.905***	.388***	.266***	-.021	.057
Safety and security				.787***	.694***	.745***	.876***	.357***	.252***	.014	.103
Human dignity					.810***	.727***	.924***	.282***	.258***	-.012	.076
Equality and equity						.587***	.902***	.222***	.204***	-.081	.056
Overall well-being harms (measured)							.752***	.453***	.392***	.092	.187***
Average well-being harm (computed)								.339***	.269***	.084	-.029
Intent to share									.321***	.177***	.094
Data sharing tax										.198***	.129*
Data sharing behaviour change (self)											.341***
Mean	3.641	3.607	3.751	3.561	3.229	3.423	3.558	3.551	25.564	78.261	47.733
Std. Dev.	0.464	0.630	0.564	0.638	0.815	0.583	0.556	0.452	8.454	24.202	19.222

Note. ***$p < .001$, **$p < .01$, *$p < .05$.

Table 2. Mean, standard deviations and correlations for the averages of all corporate vignettes (n = 302).

	Privacy	Autonomy	Safety and security	Human dignity	Equality and equity	Overall well-being harms (measured)	Average well-being harm (computed)	Intent to share	Data sharing tax	Data sharing behaviour change (self)	Data sharing behaviour change (vignette-actor)
Privacy		.686***	.685***	.646***	.517**	.645***	.800***	.443***	.417***	.215***	.080
Autonomy			.671***	.693***	.622***	.635***	.855***	.383***	.373***	.202***	.097
Safety and security				.753***	.619***	.727***	.863***	.491***	.447***	..223***	.136*
Human dignity					.780***	.747***	.911***	.485***	.532***	.267***	.212***
Equality and equity						.623***	.849***	.402***	.432***	.194***	.261***
Overall well-being harms (measured)							.786***	.563***	.521***	.280***	.229***
Average well-being harm (computed)								.511***	.514***	.256***	.193***
Intent to share									.444***	.177**	.076
Data sharing tax										.367***	.210***
Data sharing behaviour change (self)											.598***
Mean	4.405	4.205	4.062	4.030	3.910	3.423	4.122	3.680	31.501	54.676	38.245
Std. Dev.	0.484	0.631	0.593	0.637	0.744	0.583	0.530	0.555	10.619	25.093	21.118

Note. ***p < .001, **p < .01, *p <.05.

5.2 Mediation Models

For the mediation models, we calculated an average of the five distinct well-being harm dimensions; this average is called *average well-being harm*. We would argue that the calculated version of the well-being harms gives a more accurate idea of how harmful respondents found a specific behaviour since it is directly based on the five most relevant harm dimensions. Moreover, the correlations between the various well-being harms are all relatively high, suggesting that they are part of the same construct and can be used to calculate a single measure of *average well-being harm*.

Table 3 displays the outcomes of the mediation analysis for the overall model (individual vignettes); thus, the model of all individual vignettes was taken together without showing the effects of the control variables[25]. The indirect effects of both *intent to share* and *average well-being harm* on *data sharing behaviour change (self)* are significant, and in the direction we expected them to be. Hence, we can accept **H1** and **H3** for this model. However, there are no indirect effects for the model with *data sharing behaviour change (vignette-actor)*, and we, therefore, should reject **H1** and **H3** for this model. Moreover, in the model with *data sharing behaviour change (self)* as the outcome, *average well-being harm* has a significant negative direct effect. Thus, the greater the *average well-being harm* is, the smaller the behavioural change when holding the *data sharing tax* constant. This is counterintuitive and surprising.

Moreover, this seems to be a suppressed effect as the direct effect of *average well-being harm* is greater than its total effect, and the direct and indirect effects have opposite signs. *Intent to share* also still has a direct effect, but it is positive. Thus, the greater *the intent to share*, the more significant the *data sharing behaviour change (self)* when holding the *data sharing tax* constant.

Table 3. Regression coefficients from the overall mediation model for the two measurements of data sharing behaviour change (individual vignettes).

	Self	Vignette-actor
Outcome variable: *Data sharing tax*		
Average well-being harms	1.982*	1.982*
Intent to share	4.368***	4.368***
Outcome variable: *Change data sharing behaviour*		
Average well-being harms	-5.808*	1.246
Intent to share	7.250*	.184

[25] A full overview of the results (including control variables) is available as SPSS output.

Data sharing tax	.567**	.305*
Total effect: *Average well-being harms*	-4.684	1.805
Indirect effect: *Average well-being harms*	1.124 (*CI*: .009; 2.443)	.604 (*CI*: -.087; 1.568)
Total effect: *Data sharing tax*	9.727**	1.515
Indirect effect: *Data sharing tax*	2.478 (*CI*: .667; 5.052)	1.332 (*CI*: -.041; 3.339)

*Note. ***p < .001, **p < .01, *p <.05. CI stands for 95% confidence interval.*

For the corporate vignettes, the results are different. Table 4 displays the results for these models. Both indirect effects for both outcomes of *data sharing behaviour change* are significant; hence for both models, we can accept H2 and H4. Additionally, *average well-being harm* has a significant and positive direct effect on *data sharing behaviour change (vignette-actor)*.

Table 4. Regression coefficients from the overall mediation model for the two measurements of data sharing behaviour change (corporate vignettes).

	Self	Vignette-actor
Outcome variable: *Data sharing tax*		
Average well-being harms	7.816***	7.816***
Intent to share	4.637***	4.637***
Outcome variable: *Change data sharing behaviour*		
Average well-being harms	5.176	6.343*
Intent to share	-.266	-1.791
Data sharing tax	.733***	.329*
Total effect: *Average well-being harms*	10.905***	8.914**
Indirect effect: *Average well-being harms*	5.729 (*CI*: 2.755; 9.048)	2.571 (*CI*: .238; 5.112)
Total effect: *Data sharing tax*	3.133	-.266
Indirect effect: *Data sharing tax*	3.399 (*CI*: 1.176; 6.434)	1.525 (*CI*: .103; .410)

*Note. ***p < .001, **p < .01, *p <.05. CI stands for 95% confidence interval.*

5.3 Elasticity Models.

Like the mediation model, we used an average of the five distinct well-being harms and labelled this calculated variable average well-being harm. Moreover, we calculated the variable elasticity by dividing either version of *data sharing behaviour change* by *data sharing tax*. Table 5 displays the results of the multiple linear regression analysis with the two respective outcomes of elasticity as the outcome variable[26] for the individual vignettes; Table 6 shows the results for the corporate vignettes.

For the individual vignettes, *average well-being harm* has a negative effect on *elasticity (self)*. In other words, the greater the harms are, the smaller the elasticity. This is a surprising outcome and goes against **H9**. For *elasticity (vignette-actor)*, no effect can be observed. Therefore, we must reject **H9**. Also, for *intent to share*, we must reject **H10** since *intent to share* does not seem to affect either *elasticity*. We also must reject **H9** and **H10** for all models for the corporate vignettes. There is a negative effect on *data sharing behaviour change (vignette-actor)* for *intent to share*, yet this effect is negative and goes against our expectations.

Table 5. Regression coefficients of the overall model for the two types of elasticity (individual vignettes).

	Elasticity (self)			*Elasticity (vignette-actor)*		
	b	Standard error	P-value	*b*	Standard error	P-value
Average well-being harms	-2.507	1.156	.031	-1.429	.732	.052
Intent to share	< .001	1.422	> .999	-.540	.900	.549

Table 6. Regression coefficients of the overall model for the two types of elasticity (corporate vignettes).

	Elasticity (self)			*Elasticity (vignette-actor)*		
	b	Standard error	P-value	*b*	Standard error	P-value

[26] A full overview of the results (including control variables) is available as SPSS output.

Average well-being harms	-.463	.236	.051	-.266	.170	.119
Intent to share	-.158	.217	.469	-.381	.157	.016

5.4 Alternative Vignette Categorisation

To gain some detail in the analysis, we grouped the vignettes into smaller categories based on the EFA of the five well-being harm dimensions. Tables 7 and 8 display the orthogonally rotated factor solutions to the EFA on the well-being harm dimensions. We matched vignettes based on how often they had sufficiently high item loadings on the same factor from the factor solutions. The vignettes that most often and most clearly matched based on their item loadings were grouped as new vignette categories.

Table 7. Orthogonally rotated factor solutions with item loadings for each well-being harm dimension (individual vignettes).

	Factors for well-being harm dimensions											
	Privacy		Autonomy		Safety and security			Human dignity			Equality and equity	
	Factor 1	Factor 2	Factor 1	Factor 2	Factor 1	Factor 2	Factor 3	Factor 1	Factor 2	Factor 3	Factor 1	Factor 2
Data sharing affordances	.597	-.341	-.043	.641	.474	-.308	.265	.017	.546	.222	.150	.470
Location sharing	-.033	.448	.485	.172	-.027	.332	.131	.450	.298	.043	.547	.426
Disinformation spreading	.670	-.076	.093	.608	.086	.146	.723	.287	.335	.372	.481	.368
Hate speech dissemination	.667	.094	.277	.458	.211	.214	.375	.082	.087	.712	.220	.109
DNA data sharing	.350	.012	.276	.363	.528	-.172	.071	.147	.729	-.090	.205	.799
Data breaches	-.097	.553	.620	.010	.142	.639	.108	.787	-.016	.176	.776	.073
Sharing sensitive data	-.110	.554	.647	.076	.580	.132	.144	.304	-.072	.353	.702	.214
Data surveillance	-.028	.486	.525	.148	.521	.322	.073	.233	.148	.235	.539	.287
Sharing photos and videos	.189	.429	.600	.148	.693	.176	.071	.441	.303	.280	.686	.278

Table 8. Orthogonally rotated factor solutions with item loadings for each well-being harm dimension (corporate vignettes).

	Factors for well-being harm dimensions							
	Privacy		Autonomy		Safety and security		Human dignity	Equality and equity
	Factor 1	Factor 2	Factor 1	Factor 2	Factor 1	Factor 2	Factor 1	Factor 1
Data sharing affordances	.599	.083	.668	.229	.534	.347	.632	.769
Location sharing	.584	.164	.535	.206	.453	.113	.548	.579
Disinformation spreading	.223	.974	.097	.995	.183	.490	.462	.596
Hate speech dissemination	.016	.350	.271	.344	.369	.320	.599	.446
DNA data sharing	.590	.084	.686	.166	.155	.713	.505	.639
Data breaches	.663	-.060	.627	.034	.467	.134	.486	.697
Sharing sensitive data	.651	.073	.670	.186	.540	.232	.547	.582
Data surveillance	.631	.112	.546	.288	.588	.141	.645	.562
Sharing photos and videos	.425	.103	.493	.135	.364	.268	.444	.497

In the individual vignettes, we can see that the vignettes regarding *data breaches and location sharing* always load on the same factors, with the asterisk that the vignette about location sharing cross-loads for the harm dimension of equality and equity. Neither of these two vignettes shows many similarities with any other vignette, and hence we decided to pair them into a new category labelled *data breaches and location sharing*. The vignettes regarding disinformation spreading and hate speech dissemination show a similar pattern as the previous two vignettes. Hence, they most strongly load on the same factors across all well-being harm dimensions apart from equality and equity, where hate speech dissemination does not strongly load on either extracted factor. Additionally, they do not show as many similarities with any other vignettes. Therefore, we would argue that the seen pattern of shared well-being harms justifies combining them to a new vignette category labelled *hate speech and disinformation dissemination*. The vignettes about DNA data sharing and data sharing affordances share a unique pattern; they show shared solid factor loadings for the well-being harm dimensions of autonomy, human dignity, equality, and equity. They are also strongly related to the same extracted factor for privacy and safety and security dimensions, but data sharing affordances cross-loads for these dimensions. Nonetheless, we would argue that this pattern is unique enough that it allows us to combine them into one vignette category. We labelled this category *DNA and data sharing affordances*.

Lastly, the last three remaining vignettes, sharing sensitive data, data surveillance, and photo and video sharing, are clearly related based on the extracted factors for privacy, autonomy, equality, and equity. Also, for safety and security, and human dignity, their highest loadings tend to be on the same factor, yet they also do cross-load. Notably, none of the vignettes shows a similarly strong relationship with any other vignettes. Therefore, we matched them into one vignette category, called *sharing private data and data surveillance*. In summary, we detected four unique patterns of well-being harms for which we created new vignette categories.

We had hoped that the results for the corporate vignettes would be equivalent to those of the individual vignettes. However, this does not seem to be supported. In fact, the EFA does not result in any clear patterns. Notably, for human dignity and equality and equity, only a single factor was extracted, suggesting that the vignettes do not follow different patterns for these two well-being harm dimensions. Moreover, no clear patterns arise for the other three dimensions; it is somewhat visible that all vignettes also follow a similar pattern for these dimensions. Only disinformation spreading and hate speech dissemination are uniquely related to privacy and autonomy. Due to this lack of differentiation, we decided against creating smaller vignette categories and will only continue the additional analysis steps for the individual vignettes. The mediation and linear regression analyses were performed based on this categorisation. The calculation of all statistics is displayed in the following tables.

5.5 Vignette Category Models

Table 9 through Table 12 display the correlations for each vignette dimension, excluding the control variables. We can see that the sample sizes of each vignette category vary from the initial 293 observations. The reason for this variation is the same as before. Hence, in the vignette categories consisting of two or three vignettes, we have respondents who chose zero for all additional *data sharing tax* measurements, which leads to a disconnect with the measurement of *change data sharing behaviour*. Therefore, additional respondents had to be excluded from the mediation analysis and multiple linear regression for each vignette category.

Nonetheless, from the correlations, we can see that the variables seem to be related in the hypothesised direction. Hence, the *well-being harm dimensions* positively correlate with *data sharing tax* across all vignette categories. The same is true for the variable *intent to share*. Moreover, *data sharing tax* generally positively correlates with the two measurements of *change data sharing behaviour.* Notably, the correlations of *data sharing tax* with the two types of *change data sharing behaviour* - vignette-actor or self - seem to vary depending on the vignette category. For instance, for *hate speech and disinformation dissemination*, we can see a significant positive relation of *data sharing tax* with *change data sharing behaviour (self)*.
In contrast, the relation to *change data sharing behaviour (vignette-actor)* is insignificant. Contrastingly, for the vignette category of *sharing private data and data surveillance*, we see that *data sharing tax* has significant positive relations with both measures of *change data sharing behaviour*. This observation also substantiates the reorganisation of vignette categories through the EFA.

We can observe that the correlations between the five harm dimensions within each vignette category are all significant, with the Pearson coefficient ranging from minimally .150 to maximally .757. Accordingly, this also merits calculating an *average well-being harm* factor that we can use as an independent variable rather than using each manifest variable individually.

Table 9. Correlations for the vignette category *data breaches and location sharing* (n = 290).

	Privacy	Autonomy	Safety and security	Human dignity	Equality and equity	Average of well-being harm	Intent to share	Data sharing tax	Data sharing behaviour change (self)	Data sharing behaviour change actor
Privacy		.555***	.717***	.252***	.150**	.590***	.238***	.429***	.289***	.008
Autonomy			.545***	.535***	.445***	.801***	.333***	.364***	.167**	.042
Safety and security				.217***	.148**	.574***	.252***	.433***	.341***	.103
Human dignity					.784***	.850***	.223***	.136*	-.028	.020
Equality and equity						.805***	.190**	.094	-.024	.013
Average of well-being harms							.319***	.328***	.137*	.042
Intent to share								.329***	.083	-.014
Data sharing tax									.230***	-.012
Data sharing behaviour change (self)										.337***
Mean	4.660	4.324	4.714	3.545	3.459	4.140	3.512	31.103	81.029	50.640
Std. Dev.	0.527	0.765	0.520	0.987	1.102	0.590	0.654	9.501	24.301	24.360

Note. ****p* < .001, ***p* < .01, **p* <.05.

Table 10. Correlations for the vignette category of *hate speech and disinformation dissemination* (n = 276).

	Privacy	Autonomy	Safety and security	Human dignity	Equality and equity	Average of well-being harm	Intent to share	Data sharing tax	Data sharing behaviour change (self)	Data sharing behaviour change actor
Privacy		.658***	.286***	.431***	505***	.763***	-.068	.131*	-.047	.204***
Autonomy			.457***	.513***	.643***	.843***	.126*	.187**	.022	.020
Safety and security				.631**	.566***	.696***	.425***	.384***	.154*	.025
Human dignity					.765***	.814***	.349***	.374***	.190**	.016
Equality and equity						.863***	.311***	.303***	.097	.014
Average of well-being harms							.255***	.328***	.090	.078
Intent to share								.419***	.304***	-.119*
Data sharing tax									.295***	.044
Data sharing behaviour self										.037
Mean	2.587	3.426	4.539	4.033	3.772	3.689	4.596	30.980	81.576	38.121
Std. Dev.	1.144	1.074	0.765	0.870	0.931	0.764	0.651	10.798	27.876	27.174

Note. ****p* < .001, ***p* < .01, **p* <.05.

Table 11. Correlations for the vignette category of *DNA and data sharing affordances* (n = 172).

	Privacy	Autonomy	Safety and security	Human dignity	Equality and equity	Average of well-being harm	Intent to share	Data sharing tax	Data sharing behaviour change (self)	Data sharing behaviour change actor
Privacy		.757***	.703***	.718***	.693***	.877***	.650***	.439***	.054	.284***
Autonomy			.694***	.715***	.692***	.876***	.585***	.381***	.024	.262***
Safety and security				.744***	.668***	.866***	.664***	.475***	.063	.308***
Human dignity					.800***	.905***	.720***	.448***	.007	.227**
Equality and equity						.877***	.653***	.450***	.080	.251***
Average of well-being harms							.744***	.499***	.052	.302***
Intent to share								.576***	.164*	.365***
Data sharing tax									.212**	.374***
Data sharing behaviour change (self)										.482***
Mean	2.634	2.794	2.660	2.884	2.744	2.743	2.322	12.198	60.666	37.329
Std. Dev.	0.991	1.031	1.045	1.049	1.048	0.909	0.916	10.063	33.026	27.316

Note. ***p < .001, **p < .01, *p <.05.

Table 12. Correlations for the vignette category of *sharing private data and data surveillance* (n = 282).

	Privacy	Autonomy	Safety and security	Human dignity	Equality and equity	Average of well-being harm	Intent to share	Data sharing tax	Data sharing behaviour change (self)	Data sharing behaviour change actor
Privacy		.543***	.441***	.579***	.315***	.665***	.214***	256***	.284***	.183**
Autonomy			.565***	.634***	.530***	.805***	.313***	.342***	.127*	.161**
Safety and security				.601***	.656***	.837***	.265***	.332***	.022	.112
Human dignity					.629***	.850***	.245***	.350***	.143*	.134*
Equality and equity						.826***	.297***	.339***	-.017	.078
Average of well-being harms							.337***	.407***	.115	.158**
Intent to share								.327***	.098	.099
Data sharing tax									.128*	.286***
Data sharing behaviour change (self)										.456***
Mean	4.429	4.090	3.742	4.032	3.384	3.936	3.050	21.313	77.829	56.395
Std. Dev.	0.602	0.782	0.917	0.747	1.048	0.660	0.545	10.378	25.836	23.456

Note. ***p < .001, **p < .01, *p <.05.

In Table 13, we display the mean and standard deviation for the variables used in the mediation model, excluding the control variables for each vignette dimension separately. From the means, we can note that there seems to be relatively high variation between the vignette categories. In other words, depending on the vignette category, respondents gave distinct answers. The variation of scores of each variable seems to be relatively consistent independent of the vignette category. Across all variables, the lowest means always falls in the vignette category of *DNA and data sharing affordances*. The most significant *average well-being harm* can be observed for the vignette category *data breaches and location sharing*.

Similarly, the *data sharing tax* is highest for the category of *data breaches and location sharing*. For the vignette category of *hate speech and disinformation dissemination*, the means of *intent to share* and *change data sharing behaviour (self)* are higher than for any other vignette category. Lastly, for the variable *change data sharing behaviour (vignette-actor)*, the mean is highest in the category *sharing private data and data surveillance*.

Table 13. Means and standard deviations of the variables used in the mediation model for each vignette category

	Vignette Category							
	Data breaches and location sharing		*Hate speech and disinformation dissemination*		*DNA and data sharing affordances*		*Sharing private data and data surveillance*	
	Mean	Std. dev.	Mean	Std. dev.	Mean	Std. dev.	Mean	Std. dev
Average well-being harms	4.140	0.590	3.690	0.764	2.743	0.909	3.936	0.660
Intent to share	3.512	0.654	4.596	0.651	2.323	.0916	3.050	0.545
Data sharing tax	31.103	9.501	30.980	10.798	12.198	10.063	21.313	10.378
Change data sharing behaviour (vignette-actor)	50.640	24.301	38.121	27.174	37.329	27.316	56.395	23.456
Change data sharing behaviour (self)	81.029	27.360	81.576	27.867	60.666	33.026	77.829	25.836

5.6 Mediation Models of Alternative Vignette Categories

Looking at the outcomes from Table 14, we can see that in the vignette category of *data breaches and location sharing* were no indirect nor direct effects. Hence, neither *intent to share* nor *average well-being harms* affected the *change data sharing behaviour (vignette-actor)* in any way. Both independent variables were only related to the mediator *data sharing tax*. Yet also *data sharing tax* did not affect *change data sharing behaviour (vignette-actor)*. For this vignette category, we therefore should reject **H1** and **H3**.

The outcomes change in the vignette category of *hate speech and disinformation dissemination*. Again, the two independent variables have no indirect effects on *change data sharing behaviour (vignette-actor)*. Therefore, we must reject **H1** and **H3** for this vignette category. But *intent to share* has a significant direct negative effect on behavioural change. In other words, the greater the *intent to share*, the lower the *data sharing behaviour change (vignette-actor)*. This is a surprising outcome, and this also makes a suppression effect visible, where including *data sharing tax* into the model increased the negative impact of *intent to share* on *change data sharing behaviour (vignette-actor)*.

For the vignette category of *DNA and data sharing affordances*, we can accept **H3**. We see that *intent to share* indeed shows a positive indirect effect on *change data sharing behaviour (vignette-actor)*. In other words, with greater *intent to share*, the *data sharing tax* becomes higher, which ultimately leads to a more significant *change data sharing behaviour (vignette-actor)*. However, we observe no indirect effect of *average well-being harm* and, therefore, reject H1. Moreover, neither of the independent variables had a significant direct effect.

For the last vignette category, *sharing private data and data surveillance*, we can accept **H1** and **H3**. Thus, we see significant positive indirect effects for both *intent to share* and *average well-being harm*. Notably, the bootstrapping method did not infer the significance, so we used the usual theory approach. Therefore, results should be interpreted with a little extra caution. However, a higher score for both variables lead to a more significant change in the *data sharing behaviour change* for the vignette-actor via an increase in *data sharing tax*. Moreover, neither *intent to share* nor *average well-being harm* has a significant direct effect.

Table 14. Regression coefficients from the mediation model for the various vignette category with change data sharing behaviour vignette-actor as outcome.

	Data breaches and location sharing	*Hate speech and disinformation dissemination*	*DNA and data sharing affordances*	*Sharing private data and data surveillance*
Outcome variable: *Data sharing tax*				
Average well-being harms	3.276***	3.332***	1.416	4.513***
Intent to share	3.586***	4.866***	5.730***	3.933***
Outcome variable: *Change data sharing behaviour*				
Average well-being harms	1.623	3.645	.885	1.662
Intent to share	-1.138	-7.283*	5.594	-1.679
Data sharing tax	-.030	.204	.706**	.624***
Total effect: *Average well-being harm*	1.525	4.323	1.885	4.480
Indirect effect: *Average well-being harms*	-.098 (*CI*: -1.353; 1.114)	.679 (*CI*: -.476; 1.895)	1.000 (*CI*: -.399; 3.188)	2.818**
Total effect: *Intent to share*	-1.245	-6.292*	9.641**	.777
Indirect effect: *Intent to share*	-.108 (*CI*: -1.552; 1.295)	.991 (*CI*: -.531; 3.001)	4.047 (*CI*: .637; 8.261)	2.455***

*Note. ***p* < .001*, **p* < .01*, *p* <.05. *CI stands for 95% confidence interval.*

For the mediation model with *change data sharing behaviour (self*) as the outcome variable, the results change when respondents indicated their own expected behavioural change. As shown in Table 15, we can now observe a significant positive indirect effect of *intent to share* and *average well-being harm* for the vignette category *data breaches and location sharing*. Notably, neither *intent to share* nor *average well-being harm* directly affects *change data sharing behaviour (self)*. Hence, for this vignette category, we can accept **H1** and **H3**.

We now have two significant positive indirect effects for the vignette category of *hate speech and disinformation dissemination* and can therefore accept **H1** and **H3** for this category. Moreover, there is a significantly positive direct effect of *intent to share* on *change data sharing behaviour (self)* which is entirely opposite to the effect observed in the previous model. Now, greater *intent to share* will lead to a more significant change in behaviour. In other words, there appears to be a pronounced difference in the relation of the variables *intent to share* and *change data sharing behaviour* depending on whether the behavioural change concerns the self or the vignette-actor. *Average well-being harm* does not show a significant direct effect.

For the vignette category *DNA and data sharing affordances*, the results as displayed in Table 15 repeat the outcomes from Table 14. Moreover, there are no significant direct effects. Thus, we can accept **H3**, as only *intent to share* shows a significant positive indirect effect, yet *average well-being harm* does not, so we reject **H1** for this model.

Lastly, the vignette category of *sharing private data and data surveillance* now shows no significant indirect or direct effect. As for the outcomes of the vignette-actor, we had to resort to the usual theory approach, and the results should be interpreted with extra caution. But based on the outcomes, we should reject **H1** and **H3** for this vignette category. The two independent variables only seem to be related to the mediator, yet none of the variables significantly relate to *change data sharing behaviour (self)*.

Table 15. Regression coefficients from the mediation model for the various vignette category with change data sharing behaviour self as outcome.

	Data breaches and location sharing	*Hate speech and disinformation dissemination*	*DNA and data sharing affordances*	*Sharing private data and data surveillance*
Outcome variable: *Data sharing tax*				
Average well-being harms	3.276***	3.332***	1.416	4.513***
Intent to share	3.586***	4.866***	5.730***	3.933***
Outcome variable: *Change data sharing behaviour*				
Average well-being harms	2.908	-1.826	-6.119	2.175
Intent to share	-.553	9.269**	4.256	1.947
Data sharing tax	.626	.547**	.875**	.270
Total effect: *Average well-being harm*	4.958	-.004	-4.880	3.379
Indirect effect: *Average well-being harm*	2.050 (*CI*: .435; 3.987)	1.823 (*CI*: .425; 3.664)	1.238 (*CI*: -.455; 3.817)	1.204
Total effect: *Intent to share*	1.691	11.931***	9.268*	2.997
Indirect effect: *Intent to share*	2.244 (*CI*: .703; 4.257)	2.662 (*CI*: .766; 5.157)	5.012 (*CI*: 1.168; 8.736)	1.049

Note. ***p < .001, **p < .01, *p <.05. *CI stands for 95% confidence interval.*

5.7 Elasticity Models of Alternative Vignette Categories

Results of the elasticity models of vignette categories, are presented in tables 16 through 19. The tables display the results of the multiple linear regression analysis with the two respective outcomes of elasticity as the outcome variable. Again, we averaged the five distinct well-being harms to a new variable called *average well-being harm*. Moreover, we calculated the variable *elasticity* by dividing either version of *data sharing behaviour change* by *data sharing tax*.

Table 16. Regression coefficients of the vignette category *data breaches and location sharing* model for the two types of elasticity (individual vignettes).

	Elasticity (self)			*Elasticity (vignette-actor)*		
	b	Standard error	p-value	*b*	Standard error	p-value
Average well-being harms	-.935	.756	.217	-.908	.614	.140
Intent to share	-.653	.677	.335	-.525	.549	.340

Table 17. Regression coefficients of the vignette category *hate speech and disinformation dissemination* model for the two types of elasticity (individual vignettes).

	Elasticity (self)			*Elasticity (vignette-actor)*		
	b	Standard error	p-value	*b*	Standard error	p-value
Average well-being harms	-1.909	.551	< .001	-.479	.216	.027
Intent to share	.311	.700	.657	-.498	.274	.070

For the vignette category *data breaches and location sharing*, neither of the hypotheses **H9** or **H10** could be confirmed for either of the types of elasticity. Both outcomes *intent to share* and *average well-being harm* show no significant relation. We, therefore, should reject **H9** and **H10** for this model. We also should reject both hypotheses for the vignette category *hate speech and disinformation dissemination*. Moreover, contrary to our hypothesis, the effect of *average well-being harm* is negative and significant. This indicates that with greater *average well-being harm*, the *elasticity* decreases; this was found for both types of *elasticity*. Individual vignettes average well-being harm has a negative effect on both *elasticity* measures. Next, there is no significant relationship between *intent to share* or *average well-being harm* and elasticity (self) or *elasticity (vignette-actor)* for *DNA and data sharing affordances*. Consequently, we also need to reject **H9** and **H10** for this model. Lastly, for the vignette category *sharing private data and data surveillance*, we see the same results as for the category of *hate speech and disinformation dissemination*. Hence, we should reject **H9** and **H10**, and additionally, there is a significant negative effect of *average well-being harm* on both types of *elasticity*.

Table 18. Regression coefficients of the vignette category *DNA and data sharing affordances* model for the two types of elasticity (individual vignettes).

	Elasticity (self)			*Elasticity (vignette-actor)*		
	b	Standard error	p-value	*b*	Standard error	p-value
Average well-being harms	-2.634	2.569	.307	-1.110	1.522	.467
Intent to share	-4.671	2.604	.075	-2.420	1.543	.119

Table 19. Regression coefficients of the vignette category *sharing private data and data surveillance* model for the two types of elasticity (individual vignettes).

	Elasticity (self)			*Elasticity (vignette-actor)*		
	b	Standard error	p-value	*b*	Standard error	p-value
Average well-being harms	-2.689	1.168	.022	-1.948	.791	.014
Intent to share	-.645	1.362	.636	.032	.923	.972

5.8 Additional Analyses of Other Hypotheses

The results for the hypotheses **H5** through **H8** will be presented in this section. There was a significant increase in the rating of the necessity for a data pollution tax before reviewing all vignettes (M = 3.585, SD = 1.013) compared to the after they had been reviewed (M = 3.741, SD =

1.125), t(621) = -3.471, p < .001. Hence, we accept H5. There also was a significant difference in the change of behaviour for the self (M = 72.231, SD = 25.035) compared to the vignette-actor (M = 45.354, SD = 18.847), t(312) = 21.029, p < .001. Therefore, we also accept H6; respondents rated their own behavioural change as greater than the change of the vignette-actor in the individual-type vignettes. The last one-sample t-test was performed to test H7. Respondents rated their own behavioural change as a CEO of a company (M = 52.404, SD = 25.740) as higher compared to the behavioural change of the vignette-actor (M = 36.693, SD = 21.218), t(308) = 13.147, p < .001. Therefore, we accept H7.

Table 20. Multiple linear regression with *overall well-being harm* as dependent variable.

	Individual-type vignettes			Corporate-type vignettes		
	b	Std. Error	p-value	*b*	Std. Error	p-value
Privacy	.335	.072	< .001	.211	.069	.002
Autonomy	-.010	.060	.867	.084	.054	.120
Safety and Security	.379	.064	< .001	.291	.062	< .001
Human Dignity	.335	.067	< .001	.336	.067	< .001
Equality and Equity	-.105	.046	.023	.050	.049	.301

The relevant results for H8a and H8b can be seen in Table 20. We can only partly accept both hypotheses. For the individual-type vignettes, only *privacy, safety and security*, and *human dignity* are positively and significantly related to *overall well-being harm*. *Autonomy* does not show any relation, and surprisingly, *equality and equity* show a significant negative relation. Thus, the greater the harm to *equality and equity*, the smaller the *overall well-being harm*. The results of the corporate-type vignettes almost perfectly repeat the outcomes of the individual-type vignettes. Hence, *privacy, safety and security* and *human dignity* show a positive and significant relationship *with overall well-being harm*. Interestingly, now neither *autonomy* nor *equality and equity* show any relation to *overall well-being harm*.

6 Discussion and Conclusion

6.1 Overview of Findings

Our primary research question, 'should data pollution be taxed?' has been responded to with an unequivocal 'yes'. Respondents, in this study, limited to the US, clearly distinguish between some very harmful data pollution instances and those that inflict lesser harm to others. Individuals disclosing sensitive and highly personal information are penalized with the highest tax penalty ($ 33 from a maximum tax penalty of $ 40 per month). Hate speech ($ 26) and spreading disinformation ($ 26) in both individual and corporate instances are also heavily punished with tax. This thesis indisputably confirms that common forms of data transmission in which a data provider supplies data on others, substantially harms the well-being of other individuals and groups. Hence, data sharing practices that harm others, should be taxed.

We also find evidence that imposing a tax on data sharing practices will curb inflicting data pollution harms to others and change data polluter behaviour. However, we also ran into a disturbing anomaly regarding data polluters' willingness to decrease pollution behaviour. Pollution cases rated with high harm and high intent relatively showed the slightest desire to reduce polluting behaviour. We call this the 'bad behaviour paradox' and will expand on this finding below when discussing the elasticity effects of imposing a tax on data sharing behaviour.

The results of testing our hypotheses, both with ordinary regression and with the Hayes mediation model, confirms that individuals (in our case, US citizens) consider imposing a data pollution tax to be an effective measure to curb data sharing behaviour of both individuals and corporations. Indeed, our study shows that citizens are concerned that data sharing and extraction significantly affects privacy, autonomy, safety, dignity, and equality of others. In the following paragraphs, we will first address our research sub-questions. After that, we will consider significant and unexpected findings of our research that also warrant further investigation. We shall finish this thesis with some suggestions for future research and a conclusion.

6.2 Data Pollution Causes Harm to Others

Our first research sub-question queried which harms data pollution causes to others. Assessment of harm dimensions at vignette level and vignette grouping level based on factor analyses showed some interesting results and differences (Table 13). For example, DNA data sharing and spreading body-image data through Instagram were causing the most negligible harms. Hate speech and disinformation spreading ranked very high in causing overall damage. The intent to share data also shows a similar pattern. Hate speech and disinformation vignettes triggered very high scores (4,5 on a scale of 5). We can also see from Table 21 that for individual vignettes, high intent to share, combined with high harms, distinctively leads to respondents imposing incremental tax penalties. A similar pattern can be seen for corporate pollution instances, though not as pronounced as individual cases. Of interest is that this rudimentary overview of Table 21 aligns with our exploratory factor analysis results: the category of hate speech and disinformation lines up with high harms and high intent, and hence draws a relatively high tax penalty from respondents. Analogue to these findings, low harms and low intent combinations lead to reduced tax penalties.

6.3 Differences between Individual and Corporate Data Pollution

Based on our literature review in Chapter 2, we already concluded that a clear distinction should be made between data pollution activities of individuals and corporate actors, confirming our second research sub-question. The advertising revenue model underlying corporate data extraction practices has caused corporate actors to design data infrastructures addictive to data providers and contaminate information ecosystems.

Our survey respondents confirm that corporate data pollution causes greater negative externalities and higher well-being harms to others than individual data pollution. Respondents assessed harms caused by corporate actors to be substantially higher compared to individual actors (Overall Computed Harms Corporates ($M = 4.122$, $SD = 0.530$); Overall Computed Harms Individuals ($M = 3.558$, $SD = 0.556$). This rating of corporations causing relatively more significant harm with data extraction practices confirms the earlier concerns about data surveillance and extraction practices. This higher rating for corporate cases can be caused and possibly be explained by the 'status of the wrongdoer's effect' (Fragale, Rosen, Xu, & Merideth, 2009). Descriptive statistics on elasticity, defined as the relative effect of a tax penalty on expected behavioural change, shows that the individual data pollution instances show a much wider range of positive elasticities (from 1.1 to max 10.6). Interestingly, for corporate data pollution instances, elasticity hovers around an average of 1.6.

6.4 Taxonomy of Harms - Differences in Data Pollution Categories

Based on our literature review in Chapter 2, we developed a taxonomy of harms applicable to data pollution. Within that harm taxonomy, and answering our third research sub-question, we found positive and significant relationships with overall well-being harm for three harm dimensions of privacy, safety, and human dignity. However, autonomy does not show this relationship, while equality negatively correlates with overall harm. These findings require deeper analysis for the different instances of data pollution. However, due to the limited scope of this thesis, we would recommend this to be a topic of future regulatory and taxation research. We also found that respondents rated their own behavioural changes higher compared to how they assessed the vignette actors, confirming our hypotheses **H6** and **H7**. As discussed in Chapter 3, these findings corroborate earlier theories on the social desirability bias (Chung & Monroe, 2003) and the so-called 'better-than-average' effect (Zell et al., 2020)

6.5 Citizens Support a Data Pollution Tax

Regarding our fourth research sub-question, and with unambiguous support, our respondents strongly believe that data pollution should be taxed. Underwriting our predictions, our survey respondents also believe that regulators should impose a higher data pollution tax if harms and intent to share data are rated higher, confirming our primary hypotheses with just one exception. Data sharing behaviour of the vignette actor for individual vignettes did not confirm our hypothesis. We believe this can be explained by how respondents assessed the addictive nature and stickiness of social media apps, applicable to vignette actors.

Interestingly, and as could be expected based on earlier research (Ballard-Rosa, Martin, & Scheve, 2017, p. 5; Reed, 2006, pp. 725 - 726), respondents who identified themselves as having a democratic orientation scored significantly higher on overall well-being harms and the consequential data sharing tax variable. For our analyses, we also excluded respondents that indicated 'no tax' should be imposed while at the same time requiring a 100% change in behaviour. For the total sample of respondents, we excluded 20 individual vignette respondents on that basis. However, when proceeding with the more detailed analyses at vignette group levels, the number of those exclusions increased to 23 for *data breaches and location sharing*, 31 for *sharing private data and data surveillance*, 37 for *hate speech and disinformation dissemination*, and 172 for *DNA and data sharing affordances*. Due to the limited scope of this thesis, we did not analyse whether the vignettes with higher exclusions contained specific characteristics based on our demographic and other control variables.

6.6 Data Pollution Tax Changes Behaviour - Unexpectedly for Some

Our survey results, answering our fifth and final research sub-question, give rise to an unexpected and 'dark' outcome. Firstly, our work shows that a tax seems to be a suitable punishment and influences behaviour. However, contrary to our expectations, and not in line with the elasticity laws of economics on substitute goods (Chrystal & Lipsey, 1997), our results show that the greater the harms caused in some data pollution cases, the less inclined individuals were willing to change their behaviour (*data sharing behaviour change (self)*) relative to taxation. Our mediation model showed that the direct effect of well-being harms is greater than its total effect, implying that the mediating factor of tax leads to a suppression effect. The individual data pollution vignettes showed a declining elasticity of behaviour change relative to the imposed tax in instances where harms and intent were higher. We called this the 'Bad Behaviour Paradox' - the higher the damage, the lower the elasticity to change. In these instances, the intentionally caused harms motivate behaviour to the extent that it is insensitive to a tax punishment. Moreover, the elasticity model confirmed this finding when testing **H9** for individual vignettes (for both 'self' and 'vignette-actor', see Table 5) and **H10** ('vignette-actor' only, see Table 6). This paradoxid behaviour was also confirmed by the elasticity outcomes for the individual vignettes of 'Hate Speech and Disinformation Dissemination' and 'Sharing Sensitive Data and Data Surveillance'.

In our elasticity model (see Appendix B), we found that significant coefficients with negative signs suggest that if our independent variable (*well-being harms* or *intent to share*) goes up, the dependent variable (*data behaviour change*) goes down. In other words, with more significant well-being harms or intent to share, the percentage change of data sharing behaviour becomes less. Respondents do not believe that imposing a tax will curtail harmful data sharing practices.

Explanations for this nefarious behaviour can be found in the academic literature that addresses the addictive nature of social media (Andreassen, 2015; Andreassen, Pallesen, & Griffiths, 2017; Berthon, Pitt, & Campbell, 2019; Blackwell, Leaman, Tramposch, Osborne, & Liss, 2017; Craker & March, 2016; Käß, Schnürer, & Miller, 2021). Acquisti (2004) also explains the 'Bad Behaviour Paradox' partly. He supports the notion that individuals admit to more data extraction due to preferring immediate gratification and status-quo bias. The curse of immediate gratification of individual desires takes precedence. Furthermore, he suggests that rational considerations of the delayed effects of data collection on social welfare and collective well-being are disregarded by data polluters. In summary, individuals are blinded and do not recognize how their data polluting actions infringe agency, autonomy, self-directedness, and well-being of other individuals and groups.

As Cohen (1999, p. 1424) writes, 'autonomy in a contingent world requires a zone of relative insulation from outside scrutiny and interference—a field of operation within which to engage in the conscious construction of self'. If data surveillance is fully internalized, as it has become 'second nature' in constructing our social identities, the illusion of autonomy also evaporates. The concept of data pollution, operationalized in this thesis, sheds some new light on how data sharers and digital platforms impact other individuals and groups' privacy, autonomy, safety, and well-being. Around the globe, privacy debates on the level of the individual will continue. This thesis shows that next to these concerns regarding individual privacy, regulators should consider that current data sharing practices by individuals and corporations cause significant damage to others. To contain these harms to others, data pollution culprits should either be imposed with substantial tax penalties, as supported by our findings; alternatively, corporations should be required to disclose data pollution practices and be held accountable when they exceed standards, either by law or otherwise. Ultimately, if tax will not contain certain forms of data pollution sufficiently, capturing and spreading sensitive personal information should be prohibited by law.

6.7 Suggestions for Future Research

The scope of this thesis was consciously restricted to a survey that sampled respondents in the United States only. This limitation was caused by structuring tax-related measures in this study based on a US context. Extending the scope of this research to other regions would be of interest to uncover whether, for example, Europeans, Chinese, South Americans, and other areas that face significant data pollution would have survey results different from the current one. Comparing these differences would be interesting for gauging the development of a more global response to regulating data pollution. Additionally, in our research, we did not seek input from data controllers regarding their views on data pollution and taxation. Many data controllers, including social media platforms and data brokerage firms, have a vested interest in data extraction and related advertising revenues. However, eliciting the data pollution views of the data industry could contribute to developing effective regulatory measures that protect citizens from harm caused by data pollution.

Data pollution, like environmental pollution, is a global phenomenon. However, our study shows that data pollution also appears in many disguises. Behaviour modification, benefitting corporate advertising revenues, often lies at its core. Therefore, finding solutions to minimize damages, such as imposing a data pollution tax, can only become effective if mandated by global regulatory initiatives, either at United Nations or OECD level. Data pollution is highly dependent on and related to the legal concept of consent. Further research is needed to address whether legally prohibiting data categories from consent (for example, by explicitly restricting capture of specific data categories in the GDPR) would limit data transmissions and its subsequent misuse in behaviour modification practices by corporate data controllers, including social media platforms.

The ‘bad behaviour paradox’ uncovered by this study would also need deeper analyses. Could personality traits of respondents contribute to explaining these behavioural anomalies? Already, studies show that hate speech and disinformation dissemination are strongly associated with certain personality constructs, such as the Dark Triad, which implies high scores on psychopathology, narcissism, and Machiavellianism (Andreassen et al., 2017; Craker & March, 2016). Inherent manipulation sensitivities associated with personality traits also raises the question of whether the 'weak' are sufficiently protected from behaviour modification caused by data pollution. In this respect, recent and alarming research shows that children and adolescents need special attention (Boers et al., 2019; Buglass, Binder, Betts, & Underwood, 2020; Twenge et al., 2021). These unrestrained data consumers require research to better protect them from well-being harms caused by social media activities and behavioural modification.

Taxation experts often lament instrumentalism by governments, questioning whether a proposed tax measure is the realistic and only solution to the problem at hand. As (data) pollution is a normative concept (more so when considering other excise duties), it would require a consensus of what exactly data pollution entails. Consequently, governments would need objective and measurable criteria that provide a solid foundation for determining what constitutes data pollution. Therefore, more research is required to measure data pollution, which is expected to lead to numerous 'fictions' (fictive assessments, such as x % of data production is considered pollution). Fictions are common in tax legislation. However, they can also lead to regulatory tensions if the 'fiction' does not correctly represent reality. The development of data pollution measurement and fictive assertions would require further academic research. Excise duties and sin taxes are often imposed on inelastic goods - an increase in price does not significantly affect demand. Considering the earlier mentioned 'bad behaviour paradox', uncovered by this study, additional research is needed to determine how the addictive nature and stickiness of social media apps (Yujie Chen, Mao, & Qiu, 2018) can best be addressed through the design and structure of a data pollution tax. In additional research, progressive taxation to curtail excessive and harmful data pollution could be considered.

Finally, most participants in this study (517 out of some 600) indicated that they support laws setting clear limits on which data can be shared or extracted. This study provides valuable input for academics, regulators, and lawmakers on which data pollution forms inflict more significant harm and require stricter regulation. Another remarkable result of this survey is that some 500 respondents believe that big tech companies and social media platforms should have corporate reporting practices that require them to disclose data extraction practices. Finally, when asked in the survey to estimate the percentage of advertising revenues that would qualify as data pollution, participants' response was a staggering 53 %, confirming that data pollution constitutes a significant regulatory issue with potentially substantial financial and budgetary implications.

6.8 Conclusion

We have shown that data pollution appears under many disguises, affects principal data sharers, and causes significant harm to other individuals, others, groups, and so-called computed algorithmic collectives. We concur with Ben-Shahar (2019, pp. 148 - 149) when he argues that data pollution needs to be priced and taxed accordingly. Romer, a 2018 Nobel Prize winner in economic sciences, supports that notion (Romer, 2021). However, as tax experts confirm, taxation of undesirable and harmful data pollution behaviour could also signify this behaviour as being legitimate. Data pollution should be priced and measured systematically to consistently tax it. Taxation does not prohibit these dangerous activities, and a data pollution tax would only discourage behaviour by making it more expensive. Containing data pollution through taxation would also require reporting standards that would disclose the extent of corporate data pollution and the potential harms it causes. Therefore, we propose that current Corporate ESG reporting regimes provide the much-needed tools to achieve these clear objectives.

A data pollution tax, combined with enhanced corporate transparency regarding data transmission practices affecting others, will diminish information asymmetries and contribute to healthier, less addictive data sharing environments. A data pollution tax will limit well-being harms to others. Additionally, sound corporate data disclosure practices will enormously improve valuations by financial market participants of corporations that embrace ‘positive technologies’ and manage data harvesting responsibly. Timely implementation of these measures should limit behavioural modification of citizens and groups based on unjustifiable data inferences. Finally, data pollution taxation, and related disclosure practices, will strengthen the protection of critical information ecosystems and make them more resilient against assaults on their brittle equilibria.

*****

List of Tables

Appendix A

Table 21. Factor driven alternative categorization[27]:

Elasticities: Percentage Change in Behaviour / Tax %

	Individual Vignette (n = 313)	Overall Harm X Intent	Rank [28]	Tax	Rank	Behave Change Average	Rank	Actor Elasticity	Rank	Self-Elasticity	Rank	Av Elasticity	Rank [29] Av	Unique Division based on Factor Analyses
6	Robin	20,25	1	32,7	1	57,34	5	1,11	1	2,40	1	1,76	1	**Privacy & Safety and Security**
2	Julia	10,73	6	19,8	4	75,57	9	3,42	6	4,11	5	3,77	5	
1	Layla	8,18	7	6,15	8	44,71	1	4,85	8	9,69	8	7,27	8	**None**
5	Carlo	5,07	8	4,83	9	45,09	2	8,06	9	10,61	9	9,34	9	
3	Dany	19,17	2	27,25	2	53,93	3	1,15	2	2,81	2	1,98	2	**Safety & Security and Human Dignity**
4	Thierry	17,63	3	25,57	3	58,15	6	1,51	3	3,04	3	2,28	3	
8	Sabrina	4,82	9	14,36	7	71,35	8	4,69	7	5,25	7	4,97	7	**Human Dignity and Privacy**
7	Ashley	11,64	5	17,68	6	69,69	7	3,40	5	4,48	6	3,94	6	
9	Shane	12,68	4	19,06	5	54,38	4	2,00	4	3,88	4	2,94	4	
	Average	**12,24**		**18,60**		**58,80**		**3,35**		**5,14**		**4,27**		Elasticity Δ = 53%

	Corporate Vignette (n = 309)	Overall Harm X Intent	Rank	Tax	Rank	Behave Change Average	Rank	Actor Elasticity	Rank	Self-Elasticity	Rank	Av Elasticity	Rank Av	Unique Division
6	Credo	10,27	8	25,41	8	56,34	8	1,86	9	2,57	9	2,22	9	**Privacy & Safety and Security**
2	Seyu	16,11	3	28,88	6	39,74	3	1,12	3	1,63	3	1,37	3	
1	Telrot	17,07	2	34,18	1	46,99	7	1,14	4	1,61	2	1,38	4	**None**
5	Pharax	14,04	6	30,04	4	42,05	5	1,19	6	1,64	5	1,42	5	
3	Camlite	14,4	5	29,8	5	39,09	2	1,10	2	1,56	1	1,33	1	**Safety & Security and Human Dignity**
4	Clocko	17,12	1	33,21	3	45,01	6	1,07	1	1,64	4	1,36	2	
8	Google	11,61	7	26,89	7	39,76	4	1,16	5	1,80	6	1,48	6	**Human Dignity and Privacy**
7	Gray	14,47	4	33,26	2	58,59	9	1,50	8	2,02	8	1,76	8	
9	Tressor	8,82	9	19,99	9	33,00	1	1,34	7	1,96	7	1,65	7	
	Average	**13,77**		**29,03**		**44,56**		**1,28**		**1,83**		**1,55**		Elasticity Δ = 43%

[27] Numbers follow Dutch notation (commas should be read as points)
[28] Overall Harm x Intent, ranking from high (1) to low (9)
[29] Elasticity, rankings from low (1) to high (9); low ranking = low behavioural change relative to tax (increase)

Table 22. Means overview of variables to compute elasticity

	Individual (n = 313)	Pri	Aut	Saf	Dig	Equ	Overall Harm	Intent to Share	O x I[31]	Tax $ 0 - $ 40	Behaviour Change Actor	Behaviour Change Self	Behaviour Change Average	Elasticity[30] Actor	Elasticity[30] Self	Elasticity[30] Average
1	Layla - Data Sharing	1,73	2,17	2,14	2,71	2,5	2,07	3,95	8,18	6,15	29,8	59,61	44,71	4,85	9,69	7,27
2	Julia - Location Sharing	4,44	4	4,69	2,81	2,86	4,24	2,53	10,73	19,8	67,73	81,41	74,57	3,42	4,11	3,77
3	Dany - Disinfo Spreading	2,4	3,17	4,3	3,43	3,03	4,15	4,62	19,17	27,25	31,42	76,44	53,93	1,15	2,81	1,98
4	Thierry - Hate Speech	3,04	3,36	4,14	4,33	4,23	3,9	4,52	17,63	25,57	38,55	77,75	58,15	1,51	3,04	2,28
5	Carlo - DNA Sharing	2,86	2,67	2,38	2,23	2,12	1,89	2,68	5,07	4,83	38,93	51,24	45,09	8,06	10,61	9,34
6	Robin - Data Breach	4,86	4,63	4,74	4,22	3,96	4,47	4,53	20,25	32,7	36,33	78,34	57,34	1,11	2,4	1,76
7	Ashley - Sensitive Data	4,58	4,2	3,73	4,46	3,5	3,56	3,27	11,64	17,68	60,13	79,25	69,69	3,4	4,48	3,94
8	Sabrina - Data Surveil	4,41	3,9	4,01	3,89	3,34	3,42	1,41	4,82	14,36	67,28	75,41	71,35	4,69	5,25	4,97
9	Shane - Video Sharing	4,24	4,06	3,43	3,64	3,15	2,85	4,45	12,68	19,06	38,12	70,63	54,38	2	3,88	2,94
	Average	**3,62**	**3,57**	**3,73**	**3,52**	**3,19**	**3,39**	**3,55**	**12,24**	**18,60**	**45,37**	**72,23**	**58,8**	**3,35**	**5,14**	**4,27**
	Corporate (n = 309)									**% 0 - 50%**						
1	Telrot - Data Sharing	4,72	4,33	4,4	4,23	3,87	3,87	4,41	17,07	34,18	39,03	54,94	46,99	1,14	1,61	1,38
2	Seyu - Location Sharing	4,58	4,38	4,31	4,12	3,97	3,91	4,12	16,11	28,88	32,35	47,13	39,74	1,12	1,63	1,37
3	Camlite - Disinfo Spread	3,98	4,1	3,16	3,53	3,85	3,34	4,31	14,4	29,4	32,36	45,82	39,09	1,1	1,56	1,33
4	Clocko - Hate Speech	3,52	3,83	4,07	4,18	4,21	4	4,28	17,12	33,21	35,64	54,37	45,01	1,07	1,64	1,36
5	Pharax - DNA Sharing	4,56	4,17	3,72	4,18	3,71	3,5	4,01	14,04	30,04	35,7	49,3	42,5	1,19	1,64	1,42
6	Credo - Data Breach	4,83	4,4	4,62	3,96	3,83	4,39	2,34	10,27	25,41	47,36	65,32	56,34	1,86	2,57	2,22
7	Gray - Sensitive Data	4,72	4,36	4,28	4,58	4,25	4,02	3,6	14,47	33,26	49,93	67,24	58,59	1,5	2,02	1,76
8	Google - Data Surveil	4,49	4,28	4,22	3,96	3,96	3,77	3,08	11,61	26,89	31,17	48,34	39,76	1,16	1,8	1,48
9	Tressor - Video Sharing	4,18	3,91	3,74	3,41	3,38	3,01	2,93	8,82	19,99	26,81	39,18	33	1,34	1,96	1,65
	Average	**4,40**	**4,20**	**4,06**	**4,02**	**3,89**	**3,76**	**3,68**	**13,77**	**29,03**	**36,71**	**52,40**	**44,56**	**1,28**	**1,83**	**1,55**

[30] Elasticity computed as: ratio of change in behaviour (demand for data sharing) and the change in price (tax)

[31] O x I is the computed product of Overall Harm and Intent to Share

Appendix B: Overall mediation model for individual vignettes. (Colour indicates Bad Behaviour Paradox)

Overall mediation model for individual vignettes. (Colour indicates Bad Behaviour Paradox)

	H1 (harms)	H3 (intent)
Data sharing behaviour change (self)	Yes, Table 3 [1.124 (*CI*: .009; 2.443)]	Yes, Table 3 [2.478 (*CI*: .667; 5.052)]
Data sharing behaviour change (vignette-actor)	No, Table 3 [.604 (*CI*: -.087; 1.568)]	No, Table 3 [1.332 (*CI*: -.041; 3.339)]

Overall mediation model for corporate vignettes.

	H2 (harms)	H4 (intent)
Data sharing behaviour change (self)	Yes, Table 4 [5.729 (*CI*: 2.755; 9.048)]	Yes, Table 4 [3.399 (*CI*: 1.176; 6.434)]
Data sharing behaviour change (vignette-actor)	Yes, Table 4 [2.571 (*CI*: .238; 5.112)]	Yes, Table 4 [1.525 (*CI*: .103; .410)]

Overall elasticity model for individual vignettes.

	H9 (harms)	H10 (intent)
Elasticity (self)	No, Table 5 [-2.507 (p = .031)]	No, Table 5 [-.367 (p = .794]
Elasticity (vignette-actor)	No, Table 5 [-1.429 (p = .052)]	No, Table 5 [-.698 (p = .433)]

Overall elasticity model for corporate vignettes.

	H9 (harms)	H10 (intent)
Elasticity (self)	No, Table 6 [-.444 (p = .061)]	No, Table 6 [-.122 (p = .573)]
Elasticity (vignette-actor)	No, Table 6 [-.263 (p = .123)]	No, Table 6 [-.375 (p = .017)]

Alternative Vignette Categorization: Mediation Hypotheses

***Data breaches and location sharing*.**

	H1 (harms)	H3 (intent)
Data sharing behaviour change (vignette-actor)	No, Table 14 [-.098 (*CI* -1.353; 1.114)]	No, Table 14 [-.108 (*CI* -1.552; 1.295)]
Data sharing behaviour change (self)	Yes, Table 15 [2.050 (*CI* .435; 3.987)]	Yes, Table 15 [2.244 (*CI* .703; 4.257)]

Hate speech and disinformation dissemination.

	H1	H3
Data sharing behaviour change (vignette-actor)	No, Table 14 [.679 (*CI* -.476; 1.895)]	No, Table 14 [.991 (*CI* -.531; 3.001)]
Data sharing behaviour change (self)	Yes, Table 15 [1.823 (*CI* .425; 3.664)]	Yes, Table 15 [2.662 (*CI* .766; 5.157)]

DNA and data sharing affordances.

	H1	H3
Data sharing behaviour change (vignette-actor)	No, Table 14 [1.000 (*CI* -.399; 3.188)]	Yes, Table 14 [4.047 (*CI* .637; 8.261)]
Data sharing behaviour change (self)	No, Table 15 [1.238 (*CI* -.455; 3.817)]	Yes, Table 15 [5.012 (*CI* 1.168; 8.736)]

Sharing private data and data surveillance.

	H1	H3
Data sharing behaviour change (vignette-actor)	Yes, Table 14 [2.818 ($p < .05$)]	Yes, Table 14 [2.455 ($p < .05$)]
Data sharing behaviour change (self)	No, Table 15 [1.204 ($p > .05$)]	No, Table 15 [1.049 ($p > .05$)]

Alternative Vignette Categorization: Elasticity Hypotheses

Data breaches and location sharing.

	H9 (harms)	H10 (intent)
Elasticity (vignette-actor)	No, Table 16 [-.908 (p = .140)]	No, Table 16 [-.525 (p = .340)]
Elasticity (self)	No, Table 16 [-.935 (p = .217)]	No, Table 16 [-.653 (p = .335)]

Hate speech and disinformation dissemination.

	H9	H10
Elasticity (vignette-actor)	No, Table 17 [-.479 (p = .027)]	No, Table 17 [-.498 (p = .070)]
Elasticity (self)	No, Table 17 [-1.909 (p < .001)]	No, Table 17 [.311 (p = .657)]

DNA and data sharing affordances.

	H9	H10
Elasticity (vignette-actor)	No, Table 18 [-1.110 (p = .467)]	No, Table 18 [-2.420 (p = .119)]
Elasticity (self)	No, Table 18 [-2.634 (p = .307)]	No, Table 18 [-4.671 (p = .075)]

Sharing private data and data surveillance.

	H9	H10
Elasticity (vignette-actor)	No, Table 19 [-1.948 (p = .014)]	No, Table 19 [.032 (p = .972)]
Elasticity (self)	No, Table 19 [-2.689 (p = .022)]	No, Table 19 [-.645 (p = .636)]

Appendix C. Data Pollution and Taxation, Generic Questionnaire and Vignettes

Purpose of this research:
We appreciate that you are taking the time to participate in this academic research study. This is a survey on the harms caused by excessive data sharing and data extraction practices. Should these data practices be taxed at the individual level or at the corporate level? You are asked to participate in this study because your opinion matters for decisions on taxation policies.

Research procedures:
Firstly, we want to know your opinion on excessive data sharing and whether a tax should be paid on those practices. Next, we will ask you to address a number of fictional data sharing cases, 9 in total. There are no right or wrong answers for this survey. For each data sharing case, we shall query you to assess:

- Impact of data extraction on human well-being dimensions (privacy, autonomy, dignity, safety/security, and equality).
- Assessment of overall severity of those data sharing/extraction harms.
- How much tax should be levied based on your assessment of the overall severity of data sharing/extraction harms?
- If a data sharing or extraction tax is implemented, do you expect changes in data sharing behavior?

Administration and confidentiality:
Some background questions follow these queries. The questionnaire will take approximately 16 minutes, and your contribution is distinctive and essential to this research. We shall process your answers entirely anonymously. Moreover, your answers will be decoded, and we will present results only on an aggregated level without the ability to link your responses to you. Your participation is voluntary, and you may withdraw your consent and discontinue participation in this survey at any time.

Who to contact with questions:
This survey is part of a thesis and serves to complete an Executive Master's degree in Cyber Security, organised by Leiden University and Delft Technical University, both in The Netherlands. If you have any questions regarding the survey, you can contact me at h.f.m.gertsen@umail.leidenuniv.nl - I thank you for participating.

Compensation: If you complete all the answers in this survey, you shall be compensated the amount listed in the mTurk task description.

Please confirm that you participate in this survey of your own free will and that you consent to be the subject of this research. If you respond with no, you will proceed to 'end of survey', and you will not receive mTurk compensation.

Introduction to data sharing practices:
Our own data sharing, and data extraction practices by companies, can lead to the disclosure of information about others without their consent. Some of these data sharing practices go viral and cause harm to family, friends, and possibly others. The resulting information spirals can distort the delicate balances of social and political systems. Massive data breaches, disinformation campaigns, algorithmic discrimination, and sharing of DNA test data are just a few other examples of data sharing practices, harming others.

Individual or corporate data sharing cases:
This survey will present you with several instances of imagined data sharing practices of either 9 individual cases, or 9 corporate cases. Whether you get individual cases or corporate cases will be determined by chance. These cases, however, do reflect widespread data sharing practices that raise concerns with parents, teachers, politicians, scientists, and society at large.

Question formats:
Please note that we ask you to respond to each question to the best of your knowledge. Some of the questions require you to move a slider on a given scale. Be aware that you need to actively move the slider on the scale to the position you believe is correct to properly respond to the question.

Data Pollution Vignette Questions in Generic Format

Q1 Please confirm that you participate in this survey of your own free will and that you consent to be the subject of this research. If you respond with no, you will proceed to 'end of survey', and you will not receive mTurk compensation.

Q2. Currently, I believe that levying a tax on harmful data sharing and data extraction practices will decrease data transmissions.
(Scale from strongly disagree - to strongly agree: Likert 5)

Detailed Questions for each Vignette: **Individual Actors:**

Q3. When individual actor x is sharing data through instrument y, I believe that individual actor x will affect well-being of other individuals z, in the following manner:

- Privacy will be impaired (not at all - to fully: Likert 5)
- Autonomy will be diminished (not at all - to fully: Likert 5)
- Safety and security will be put at risk (not at all - to fully: Likert 5)
- Human dignity will be harmed (not at all - to fully: Likert 5)
- Equality will be damaged (not at all - to fully: Likert 5)

Q4. Based on the previous grading of potential harms caused by individual actor x, I believe that the overall harm caused by actor x can be qualified as: (Scale: no harms/not severe - to very significant harms; Likert 5)

Q5. I believe that individual actor x, when using instrument y, intended to share data to the following extent: (Scale: No intention to share at all - to full intention to share with many; Likert 5)

Q6. If a personal data sharing tax is levied on actor x for activities using instrument y, I believe that actor x should pay the additional $ amount of taxes through actor's monthly internet billing: (amount scale: from $ 0 - to $ 40)

Q7. If data sharing of actor x through instrument y is taxed according to (**Q6**), then I believe actor x will decrease the data sharing activities to the following extent (no change in data sharing behaviour at all - to completely stop sharing behaviour: Scale 0 to 100%)
Q8. If I would use instrument y, and I would be taxed according to (**Q6)**, I would decrease my data sharing behaviour to the following extent (no change in data sharing behaviour at all - to completely stop sharing behaviour: Scale 0 to 100%)

Corporate Actors (same structure as individual actors):

Q9. When corporate actor A is sharing data through instrument B, I believe that corporate actor A will affect well-being of other individuals C, in the following manner:

- Privacy will be impaired (not at all - to fully: Likert 5)
- Autonomy will be diminished (not at all - to fully: Likert 5)
- Safety and security will be put at risk (not at all - to fully: Likert 5)
- Human dignity will be harmed (not at all - to fully: Likert 5)
- Equality will be damaged (not at all - to fully: Likert 5)

Q10. Based on the previous grading of potential harms caused by corporate actor A, I believe that the overall data sharing/extraction harms caused by actor A can be qualified as: (Scale: no harms/not severe - to very significant harms; Likert 5)

Q11. I believe that corporate actor A, when using instrument B, intended to share/extract data to the following extent: (Scale: No intention to share at all - to full intention to share with many; Likert 5)

Q12. If an additional corporate tax is levied on profits of data sharing by corporate actor A, for activities using instrument B, I believe that corporate actor A should pay the following incremental tax: (percentage additional tax on data sharing profits - scale from 0% to 50%)

Q13. If profits of data sharing activities through (instrument B) of corporate actor A are taxed with incremental tax according **to Q12**, then I believe corporate actor A will decrease the data sharing/extraction activities to the following extent: (no change in data sharing/extraction behaviour at all - to completely stop sharing behaviour: Scale 0 to 100%)

Q14. If I would be the CEO of corporate actor A, and the corporation would be taxed according to (**Q12**), as CEO, I would decrease data sharing/extraction behaviour of corporate actor A to the following extent (no change in data sharing/extraction behaviour at all - to completely stop sharing behaviour: Scale 0 to 100%)

Questions after Detailed Vignette Questions:

Q15.Considering the case studies I have now responded to in this survey, I currently believe that harmful data sharing and data extraction practices will be decreased by levying a tax?
(Scale from strongly disagree - to strongly agree: Likert 5)

Q16. Social media platforms, and related companies, derive substantial amounts of revenues from advertising income. Based on your own experience and knowledge of data sharing practices, what is the percentage (%) of advertising income you believe can be attributed to data pollution activities (or excessive data extraction) by these companies on average? Scale from 0% to 100%.

Q17. Which of the following measures would you support to resolve excessive data sharing and data extraction practices? You can select more than one answer.

- Set clear limits in law which data can be shared or extracted
- The internet society should regulate data sharing practices
- Big Tech companies and social media platforms should have reporting practices and standards in place that require them to disclose data extraction practices
- There should be a global (UN based) data protection authority
- Other measures you would support (free format text as response)

Demographic Questions:

Q18. Please indicate your gender (male, female, non-binary/third gender, prefer not to say).

Q19. Please indicate your age.

Q20. How would you describe your ethnicity (5 choices)?

Q21. Which category best describes your highest level of education attained (7 choices)?

Q22. Which political party did you vote for during the presidential election in 2020? If you were not able to vote, just choose the party you wanted to win the election at that time. (Republican, Democratic, Other, do not prefer to answer).

******

Individual Vignettes:

1. Layla: Instagram Body Image Dissatisfaction (Data Sharing Affordances)
Layla, a female adolescent, and college student, visits the gym at least four times a week. One of her passions is to become a fashion model. Layla is very active on Instagram with hundreds of friends. She enjoys getting 'likes' from and giving 'likes' to as many friends as possible. Layla uploads many selfies of her sporting activities and enjoys showing that she is in excellent shape - ready to become a fashion model. A lot of Layla’s friends feel pressured to also engage in sporting activities. However, many of them lack the energy (and time) needed to exercise. The constant comparison with Layla’s ‘perfection’ causes her friends to feel unhappy with their current body weight and shape. A growing number of Layla’s friends try rigorous diets as an alternative to getting in shape. (134 words)

2. Julia: Strava Location Sharing and Tracking (Location Sharing)
Julia, a lieutenant with the US marines, uses Strava (a fitness and location tracking app) to record her running activities. Competitive as she is, she has invited many colleagues and friends to follow her on Strava. Recently, she has been seconded to a secret NATO military operation in Tajikistan, a country in Central Asia. Running tracks around her camp on the foot of the Pamir mountains are rare and are based on paths used by shepherds, smugglers, and other soldiers. For safety reasons, the US soldiers often exercise together. By using the fitness app, Julia has contributed to information that clusters physical workouts of herself and her colleagues at the base of the Pamir mountains. These ‘heatmaps’ on Strava disclose the location information of US marines abroad. (127)

3. Dany: Covid Disinformation Spreading (Disinformation Spreading)
Dany, a civil engineer by training, is a productive Covid anti-vaccine activist. Measured by the number of followers on his weblog, he ranks with the top 20 influential anti-vaxxers. He has repeatedly posted false Covid vaccine information on his blog with cross-postings to social media accounts, all with the sole purpose of increasing the number of followers. Dany knows that incorrect information travels faster and broader into the social media networks compared to genuine content. His disinformation on the vaccines has confused many individuals in their vaccine decision-making process and may have caused additional Covid deaths. (96)

4. Thierry: Hate Speech (Hate Speech Dissemination)
As an unemployed electrician, Thierry has plenty of time to participate in weblogs. In those blogs, he consistently blames certain groups of individuals for causing his unfortunate career stop. He believes that the influx of well-educated refugees from war-ridden neighbouring countries has triggered his unemployment. Thierry has also taken the lead in some very active hate speech groups that target refugees. He relentlessly cross-posts many of his conversations on a variety of social media platforms and forums. Thierry’s words may influence the way people look at refugees. (87)

5. Carlo: DNA Data Sharing (DNA Data Sharing)
Carlo, a grandfather of six, recently retired and could finally pursue a long-time interest to find out more about his family history. As he suffers from a rare genetic condition that leads to paralysis, he has been in a wheelchair now for five years. Recently, he subscribed to a website dedicated to ancestry and purchased a DNA test. Based on his genetic data and other information shared by Carlo, this site allowed him to find many ancestors. Carlo could also connect and communicate with hundreds of first, second and even third-degree nephews and nieces worldwide. He actively pursued this possibility, often to the surprise of these (far-out) relatives. Many of these DNA-based contacts were shocked to learn about Carlo’s genetic disorder and worried about their medical condition and family members. (130)

6. Robin: Enabling Data Breach (Data Breaches)
Robin participates in an online forum that discusses techniques to collect personal data from active individuals on social media platforms. Recently, and with some help from experts who know how to gather data on the internet, he obtained a massive data file containing the personal information of over 500 million Facebook users from some 100 countries. For a small fee, Robin has now made that file available on the internet, including users' phone numbers, Facebook ID's, full names, locations, birthdates, and some email addresses. (84)

7. Ashley: Sexual Conversation Screenshot Sharing (Sharing Sensitive Data)
Ashley recently moved from a rural area where she attended college to San Francisco. Eager to make new friends, she subscribed to a popular dating platform and shared data from her other social media apps with this new app. After a few months, Ashley got very attracted to a new friend who shared many interests. They enjoyed lots of passions together, including sports activities, wining and dining, and sexual experimentation. To show off to other friends, Ashely took several 'hot' screenshots of sexual conversations with her lover and communicated those with other friends on social media. After posting, some of Ashley's screenshots went viral. (104)

8. Sabrina: Sharing Sensitive Client Data by Gmail (Data Surveillance)
Sabrina uses Gmail as her first-choice email system; it is free of charge and always available. She has a successful career as a psychotherapist and consults some 30 clients monthly. Sabrina shares her diagnoses and therapy suggestions with her clientele through Gmail and stores her client data in the cloud. Sabrina has not installed end-to-end email encryption and is unaware that Google scans the email traffic relating to her psychotherapy activities. These emails contain sensitive personal information about Sabrina's clients. (80)

9. Shane: Picture Sharing Music Festivals (Photo and Video Sharing)
Shane, a photography student, is interested in how faces express emotions. He shares most of his pictures with his extensive social network, including his colleague students, family, and friends. He takes many of his photographs at big music festivals where thousands of music fans attend. As a photographer, Shane is proud of his artistic work. Many of his pictures are tagged by festival attendees and spread over social media networks almost virally. Following the atmosphere at these festivals, many of his 'facial expressive' shots expose the intimate feelings of the participants. After the festival, Shane ignores requests by individuals to remove images from his social media accounts. He argues that his work is that of an artist. (117; average 107)

*****

Corporate Vignettes:

1. TELROT: Background Data Profiling (Data Sharing Affordances)
TELROT, a data analytics company, has developed some 150 data collection apps. These apps enable TELROT to gather sensitive profile information of individuals that use social media. Tom is an active user of social media, and he is networking with many friends and relatives. Through the TELROT apps, many of Tom's connections share personal and privacy-sensitive data of him. As the data-hungry TELROT apps primarily operate in the background, Tom's friends are unaware of transmitting sensitive information. The data includes photos and videos, current location and profile data of Tom, his family, friends, and other relationships. Tom has many friends; he is neither aware of this data sharing through TELROT nor has he consented to his friends to share his data. TELROT sells the profile data of Tom, his family and friends and generates substantial revenues from these hidden data collection practices. (142 words)

2. SEYU: Location Data Sharing (Location Sharing)
SEYU, a (fictitious) major mobile phone operator, collects customer location data. SEYU also arranged that some of the largest data brokers in the country provide SEYU with other personally identifiable information of its customers. Subsequently, SEYU sells the enriched location data to bounty hunters who use it to locate fugitives, people who have not paid their mortgage instalments, and individuals in default on car payments. SEYU also supplies similar data to the Immigration and Customs agency, which use the information to locate people designated for deportation. SEYU also shared the exact location data with the tax authorities to unravel schemes of money laundering. Selling enriched location data is a very profitable business for SEYU. (114)

3. CAMLITE: Political Misinformation Spreading (Disinformation Spreading)
In the wake of forthcoming presidential elections, CAMLITE, a political advertising company, got access to the personal data of Facebook users and provided these users with data-driven advertisements. CAMLITE constructed these ads carefully, and they contained polarizing political information on election candidates that could influence voting behavior. CAMLITE specialises in behavior modification and knows how to influence voters at both conscious and unconscious levels. Based on social media data, CAMLITE directed advertisements at individuals who were still in doubt on who to vote. In making up their minds, these ads caused many voters to doubt their traditional political party preferences. (100)

4. CLOCKO: Spreading Discriminatory Messages (Hate Speech Dissemination)
CLOCKO (a fictitious company) is a corporation building websites for political parties, some with extreme views. Computational advertising academics founded CLOCKO and these scientists know how to exploit human biases to maximise political propaganda. An extremist political party used CLOCKO's manipulative powers to convince voters and ensure that its polarising views prevailed. The party paid CLOCKO substantial amounts. Cleverly disguising the extremist nature of the political group, CLOCKO built several websites for the politicians. Predictably, CLOCKO's websites acted as catalysts in spreading discriminatory messages about specific minority groups of society by utilising social media reinforcement mechanisms. (96)

5. PHARAX: DNA Data Advertising (DNA Data Sharing)
PHARAX purchases genetic information of individuals who used consumer DNA tests without obtaining these consumers' consent. PHARAX is a successful pharmaceutical multinational specialising in treating a rare disease based on a genetic deficiency. The condition can be treated best with daily medication. Marketing its product is only cost- effective when PHARAX can approach potential customers directly. For that reason, PHARAX combines the DNA data they acquired with email addresses and social media identifiers obtained from data brokers. By combining all this

information, PHARAX can now target its potential consumers with dedicated advertisements for medical treatment. These ads have caused many individuals anxiety because of the unexpected and unknown exposure to the rare genetic condition. PHARAX has generated substantial additional profits from its aggressive individual advertising campaigns using DNA data. (129)

6. CREDO: Consumer Credit Data Breach (Data Breaches)
The databases of CREDO, a large credit reporting company, were compromised. Sensitive personally identifiable information of over 150 million individuals was misappropriated. The files with the stolen data were offered for sale on the dark web. Within minutes, numerous transactions were executed, and many organisations got hold of the personal information of CREDO's credit consumers. Following this massive data breach, CREDO's customers have started class-action suits. Their personal information has been compromised and is now accessible to whoever is interested. In essence, CREDO failed to protect its data systems, containing sensitive consumer credit information of a very large number of people. (101)

7. GRAY: HIV Data Sharing (Sharing Sensitive Data)
GRAY, a well-known gay dating app with some 4 million daily users across the globe, allows its customers to include their HIV status and ‘last tested date’ into their profiles. This information, together with the app user’s location data, phone ID and email addresses have been shared by GRAY with a few other companies without notifying its app users. When GRAY customers found out that the app company was selling their HIV data to other companies, they were agitated. Many GRAY users decided to withhold highly sensitive HIV status information. However, because of not disclosing HIV related information, many of GRAY’s users are now treated with suspicion and are considered less attractive dating partners. (114)

8. Google Docs: Leaking Activist Data (Data Surveillance)
Recently, climate activists in a country in the southern hemisphere, protested new agricultural laws that would further impair the delicate environmental balance in their country. A group of activists set up a protest and worked as a team on a pamphlet explaining their concerns with the proposed changes of the new law. The activists used Google Docs for creating and editing their flyers. Before the protest, the police arrested several activists and accused them of setting up riots. Some of the protesters are still in jail. The protesters assert that the police could identify them because Google shared the data of the activists located on Google Docs with the police. The conditions under which the police got hold of the protesters’ Google Docs data remain unclear. (126)

9. TRESSOR: Bystander Video Sharing (Photo and Video Sharing)
TRESSOR, the market leader for police body cams, collects, stores and analyses data of all the body cams worn by police agents. TRESSOR has an exclusive contract with the US police to analyse the videos, also using facial recognition techniques. TRESSOR has shared these body cam data files related to political protest happenings with the Justice Department in some states. Studying these files, the Justice Department identified innocent bystanders appearing in these videos. To their surprise, and causing them anxiety, the Justice Department approached them to testify in some of the cases involving riots during these protests. (97; average 113)

*****

Data Pollution and Taxation

Acemoglu, D., Makhdoumi, A., Malekian, A., & Ozdaglar, A. (2019). *Too much data: Prices and inefficiencies in data markets* (0898-2937). Retrieved from https://www.nber.org/papers/w26296

Acquisti, A. (2004). *Privacy in electronic commerce and the economics of immediate gratification.* Paper presented at the Proceedings of the 5th ACM conference on Electronic commerce.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature, 54*(2), 442-492. doi:10.1257/jel.54.2.442

Albury, K., Burgess, J., Light, B., Race, K., & Wilken, R. (2017). Data cultures of mobile dating and hook-up apps: Emerging issues for critical social science research. *Big Data & Society, 4*(2), 2053951717720950.

Alexander, C. S., & Becker, H. J. (1978). The use of vignettes in survey research. *Public opinion quarterly, 42*(1), 93-104.

Alicke, M. D., & Govorun, O. (2005). The better-than-average effect. *The self in social judgment, 1*, 85-106.

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of economic Perspectives, 31*(2), 211-236.

Andreassen, C. S. (2015). Online social network site addiction: A comprehensive review. *Current Addiction Reports, 2*(2), 175-184.

Andreassen, C. S., Pallesen, S., & Griffiths, M. D. (2017). The relationship between addictive use of social media, narcissism, and self-esteem: Findings from a large national survey. *Addictive behaviors, 64*, 287-293.

Arechar, A. A., Kraft-Todd, G. T., & Rand, D. G. (2017). Turking overtime: how participant characteristics and behavior vary over time and day on Amazon Mechanical Turk. *Journal of the Economic Science Association, 3*(1), 1-11.

Athey, S., Catalini, C., & Tucker, C. (2017). *The digital privacy paradox: Small money, small costs, small talk* (0898-2937). Retrieved from

Atzmüller, C., & Steiner, P. M. (2010). Experimental vignette studies in survey research. *Methodology*.

Avraham, R. (2018). Personal Data as an Environmental Hazard. *Jotwell: J. Things We Like*, 1.

Babcock, A. F. (2021). Laws and Taxes and Big Tech, Oh My! The Case for a Federal Excise Tax on Targeted Digital Advertisements Created by Use of Personally Identifiable Data. *Wash. UL Rev., 99*, 271.

Baig, K., Mohamed, R., Theus, A.-L., & Chiasson, S. (2020). *" I'm hoping they're an ethical company that won't do anything that I'll regret" Users Perceptions of At-home DNA Testing Companies.* Paper presented at the Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems.

Bail, C. A., Argyle, L. P., Brown, T. W., Bumpus, J. P., Chen, H., Hunzaker, M. F., . . . Volfovsky, A. (2018). Exposure to opposing views on social media can increase political polarization. *Proceedings of the National Academy of Sciences, 115*(37), 9216-9221.

Bakhiyi, B., Gravel, S., Ceballos, D., Flynn, M. A., & Zayed, J. (2018). Has the question of e-waste opened a Pandora's box? An overview of unpredictable issues and challenges. *Environment international, 110*, 173-192.

Balkin, J. M. (2020). *The Fiduciary Model of Privacy.* Paper presented at the Harvard Law Review Forum.

Ballard-Rosa, C., Martin, L., & Scheve, K. (2017). The structure of American income tax policy preferences. *The Journal of Politics, 79*(1), 1-16.

Barendt, E. (2019). What is the harm of hate speech? *Ethical Theory and Moral Practice, 22*(3), 539-553.

Barocas, S., & Levy, K. (2020). Privacy dependencies. *Wash. L. Rev., 95*, 555.

Barratt, P. (2017). Healthy competition: A qualitative study investigating persuasive technologies and the gamification of cycling. *Health & place, 46*, 328-336.
Batiste-Boykin, C. (2015). In re Google Inc.: ECPA, consent, and the ordinary course of business in an automated world. *Intell. Prop. L. Bull., 20*, 21.
Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. (2014). After Snowden: Rethinking the impact of surveillance. *International political sociology, 8*(2), 121-144.
Baumol, W. J. (1972). On taxation and the control of externalities. *The American economic review, 62*(3), 307-322.
Beam, M. A., Hutchens, M. J., & Hmielowski, J. D. (2018). Facebook news and (de) polarization: reinforcing spirals in the 2016 US election. *Information, Communication & Society, 21*(7), 940-958.
Ben-David, A., & Fernández, A. M. (2016). Hate speech and covert discrimination on social media: Monitoring the Facebook pages of extreme-right political parties in Spain. *International Journal of Communication, 10*, 27.
Ben-Shahar, O. (2019). Data Pollution. *Journal of Legal Analysis, 11*, 104-159. doi:10.1093/jla/laz005
Ben-Shahar, O., & Schneider, C. E. (2014). *More than you wanted to know;The Failure of Mandated Disclosure*: Princeton University Press.
Bergemann, D., Bonatti, A., & Gan, T. (2019). The economics of social data.
Berthon, P., Pitt, L., & Campbell, C. (2019). Addictive de-vices: A public policy analysis of sources and solutions to digital addiction. *Journal of Public Policy & Marketing, 38*(4), 451-468.
Bietti, E., & Vatanparast, R. (2020). Data Waste. *Harvard International Law Journal, 61*.
Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). *Third party tracking in the mobile ecosystem.* Paper presented at the Proceedings of the 10th ACM Conference on Web Science.
Blackwell, D., Leaman, C., Tramposch, R., Osborne, C., & Liss, M. (2017). Extraversion, neuroticism, attachment style and fear of missing out as predictors of social media use and addiction. *Personality and individual differences, 116*, 69-72.
Boers, E., Afzali, M. H., Newton, N., & Conrod, P. (2019). Association of screen time and depression in adolescence. *JAMA pediatrics, 173*(9), 853-859.
Boley, H., & Chang, E. (2007). *Digital ecosystems: Principles and semantics.* Paper presented at the 2007 Inaugural IEEE-IES Digital EcoSystems and Technologies Conference.
Brady, W. J., Wills, J. A., Jost, J. T., Tucker, J. A., & Van Bavel, J. J. (2017). Emotion shapes the diffusion of moralized content in social networks. *Proceedings of the National Academy of Sciences, 114*(28), 7313-7318.
Braillon, A. (2012). Taxing "Sin drinks": From economy to sugar control. *Preventive medicine, 3*(54), 283.
Brandeis, L., & Warren, S. (1890). The right to privacy. *Harvard law review, 4*(5), 193-220.
Brandtzaeg, P. B., Pultier, A., & Moen, G. M. (2019). Losing control to data-hungry apps: A mixed-methods approach to mobile app privacy. *Social Science Computer Review, 37*(4), 466-488.
Buglass, S. L., Binder, J. F., Betts, L. R., & Underwood, J. D. (2020). Asymmetrical third-person effects on the perceptions of online risk and harm among adolescents and adults. *Behaviour & information technology*(March 2020), 1-11.
Buntain, C., Bonneau, R., Nagler, J., & Tucker, J. A. (2021). YouTube recommendations and effects on sharing across online social platforms. *Proceedings of the ACM on Human-Computer Interaction, 5*(CSCW1), 1-26.
Burton, J. W., Cruz, N., & Hahn, U. (2021). Reconsidering evidence of moral contagion in online social networks. *Nature human behaviour*, 1-7.
Cai, K.-Y., & Zhang, C.-Y. (1996). *Towards a research on information pollution.* Paper presented at the 1996 IEEE International Conference on Systems, Man and Cybernetics. Information Intelligence and Systems (Cat. No. 96CH35929).

Caminker, E. (2019). Location Tracking and Digital Data: Can Carpenter Build a Stable Privacy Doctrine? *The Supreme Court Review, 2018*(1), 411-481.

Capra, F., & Luisi, P. L. (2014). *The systems view of life: A unifying vision*: Cambridge University Press.

Carattini, S., Kallbekken, S., & Orlov, A. (2019). How to win public support for a global carbon tax. In: Nature Publishing Group.

Carlsson, B. (2004). The Digital Economy: what is new and what is not? *Structural change and economic dynamics, 15*(3), 245-264.

Chan, T. K., Cheung, C. M., & Wong, R. Y. (2019). Cyberbullying on social networking sites: The crime opportunity and affordance perspectives. *Journal of Management Information Systems, 36*(2), 574-609.

Chen, A. (2019). From attachment to addiction: the mediating role of need satisfaction on social networking sites. *Computers in Human Behavior, 98*, 80-92.

Chen, Y., Mao, Z., & Qiu, J. L. (2018). *Super-sticky WeChat and Chinese society*: Emerald Group Publishing.

Chen, Y., Sherren, K., Smit, M., & Lee, K. Y. (2021). Using social media images as data in social science research. *New Media & Society*, 14614448211038761.

Cheng, J., Adamic, L., Dow, P. A., Kleinberg, J. M., & Leskovec, J. (2014). *Can cascades be predicted?* Paper presented at the Proceedings of the 23rd international conference on World wide web.

Cheng, J., Bernstein, M., Danescu-Niculescu-Mizil, C., & Leskovec, J. (2017). *Anyone can become a troll: Causes of trolling behavior in online discussions.* Paper presented at the Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing.

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior, 81*, 42-51.

Choi, J. P., Doh-Shin, J., & Byung-Cheol, K. (2019). Privacy and personal data collection with information externalities. *Journal of Public Economics, 173*, 113-124.

Choi, S., & Kim, E.-M. (2020). Between Instagram browsing and subjective well-being: Social comparison or emotional contagion? *Media psychology*, 1-25.

Christakis, N. A., & Fowler, J. H. (2009). *Connected: The surprising power of our social networks and how they shape our lives*: Little, Brown Spark.

Christakis, N. A., & Fowler, J. H. (2013). Social contagion theory: examining dynamic social networks and human behavior. *Statistics in medicine, 32*(4), 556-577.

Chrystal, K. A., & Lipsey, R. G. (1997). Economics for business and management. *OUP Catalogue*.

Chung, J., & Monroe, G. S. (2003). Exploring social desirability bias. *Journal of Business Ethics, 44*(4), 291-302.

Claesson, A., & Bjorstad, T. (2020). *"Out of Control' - A Review of Data Sharing by Popular Mobile Apps*. Retrieved from Oslo:

Cobb, C., & Kohno, T. (2017). *How public is my private life? Privacy in online dating.* Paper presented at the Proceedings of the 26th International Conference on World Wide Web.

Cockfield, A., Hellerstein, W., & Lamensch, M. (2019). *Taxing global digital commerce*: Kluwer Law International BV.

Codagnone, C., & Martens, B. (2016). Scoping the sharing economy: Origins, definitions, impact and regulatory issues. *Cristiano Codagnone and Bertin Martens (2016). Scoping the Sharing Economy: Origins, Definitions, Impact and Regulatory Issues. Institute for Prospective Technological Studies Digital Economy Working Paper, 1*.

Cohen, J. E. (1999). Examined lives: Informational privacy and the subject as object. *Stan. L. Rev., 52*, 1373.

Connolly, N. (2015). CSR is dead: long live Pigouvian taxation. *The International Journal of Human Rights, 19*(6), 849-866.

Conole, G., & Dyke, M. (2004). Understanding and using technological affordances: a response to Boyle and Cook. *ALT-J, 12*(3), 301-308.

Couldry, N. (2019). Capabilities for what? Developing Sen's moral theory for communications research. *Journal of Information Policy, 9*, 43-55.
Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*: Stanford University Press.
Craker, N., & March, E. (2016). The dark side of Facebook®: The Dark Tetrad, negative social potency, and trolling behaviours. *Personality and individual differences, 102*, 79-84.
Cui, W. (2019). The digital services tax: a conceptual defense. *Tax L. Rev., 73*, 69.
Daniel, P., Krupnick, A., Matheson, M. T., Mullins, P., Parry, I., & Swistak, A. (2017). *How should shale gas extraction be taxed?* : International Monetary Fund.
Daniels, J. (2009). Cloaked websites: propaganda, cyber-racism and epistemology in the digital era. *New Media & Society, 11*(5), 659-683.
de Brouwer, S. (2019). *Privacy Self-Management and the Issue of Privacy Externalities: Managing One's Privacy Badly, and Others' Even Worse.* (Master). Utrecht University,
de Brouwer, S. (2020). Privacy self-management and the issue of privacy externalities: Of thwarted expectations, and harmful exploitation. *Internet Policy Review, 9*(4), 1-29.
de Reuver, M., Sørensen, C., & Basole, R. C. (2018). The digital platform: a research agenda. *Journal of Information Technology, 33*(2), 124-135.
de Vries, D. A., Möller, A. M., Wieringa, M. S., Eigenraam, A. W., & Hamelink, K. (2018). Social comparison as the thief of joy: Emotional consequences of viewing strangers' Instagram posts. *Media psychology, 21*(2), 222-245.
Deibert, R. (2020). Reset: Reclaiming the internet for civil society. *Toronto, ON: House of Anansi*.
Del Vicario, M., Bessi, A., Zollo, F., Petroni, F., Scala, A., Caldarelli, G., . . . Quattrociocchi, W. (2016). The spreading of misinformation online. *Proceedings of the National Academy of Sciences, 113*(3), 554-559.
Deutskens, E., De Ruyter, K., Wetzels, M., & Oosterveld, P. (2004). Response rate and response quality of internet-based surveys: an experimental study. *Marketing letters, 15*(1), 21-36.
DeVito, M. A., Birnholtz, J., & Hancock, J. T. (2017). *Platforms, people, and perception: Using affordances to understand self-presentation on social media.* Paper presented at the Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing.
Diamond, P. A., & Mirrlees, J. A. (1971). Optimal taxation and public production I: Production efficiency. *The American economic review, 61*(1), 8-27.
Donovan, J., & Boyd, D. (2021). Stop the presses? Moving from strategic silence to strategic amplification in a networked media ecosystem. *American Behavioral Scientist, 65*(2), 333-350.
Dow, P. A., Adamic, L. A., & Friggeri, A. (2013). *The anatomy of large facebook cascades.* Paper presented at the Seventh international AAAI conference on weblogs and social media.
Dumas, T. M., Maxwell-Smith, M. A., Tremblay, P. F., Litt, D. M., & Ellis, W. (2020). Gaining likes, but at what cost? Longitudinal relations between young adults' deceptive like-seeking on instagram, peer belonging and self-esteem. *Computers in Human Behavior, 112*, 106467.
Dunn, R. (2021). *A Natural History of the Future: What the Laws of Biology Tell Us about the Destiny of the Human Species*: Hachette UK.
Dwyer, R., & Fraser, S. (2016). Addicting via hashtags: How is Twitter making addiction? *Contemporary Drug Problems, 43*(1), 79-97.
Edenhofer, O., Franks, M., & Kalkuhl, M. (2021). Pigou in the 21st Century: a tribute on the occasion of the 100th anniversary of the publication of The Economics of Welfare. *International Tax and Public Finance*, 1-32.
Egele, M., Kruegel, C., Kirda, E., & Vigna, G. (2011). *PiOS: Detecting Privacy Leaks in iOS Applications.* Paper presented at the NDSS.
Evans, D. S. (2012). Governing bad behavior by users of multi-sided platforms. *Berkeley Tech. LJ, 27*, 1201.
Fairfield, J. A., & Engel, C. (2015). Privacy as a public good. *Duke LJ, 65*, 385.

Feinstein, B. A., Hershenberg, R., Bhatia, V., Latack, J. A., Meuwly, N., & Davila, J. (2013). Negative social comparison on Facebook and depressive symptoms: Rumination as a mechanism. *Psychology of Popular Media Culture, 2*(3), 161.

Fenwick, M., McCahery, J. A., & Vermeulen, E. P. (2019). The end of 'corporate'governance: hello 'platform'governance. *European Business Organization Law Review, 20*(1), 171-199.

Ferrara, E. (2017). Contagion dynamics of extremist propaganda in social networks. *Information Sciences, 418*, 1-12.

Ferrara, E., Cresci, S., & Luceri, L. (2020). Misinformation, manipulation, and abuse on social media in the era of COVID-19. *Journal of Computational Social Science, 3*(2), 271-277.

Feygin, Y., Li, H., Lala, C., Hecht, B., Vincent, N., Scarcella, L., & Prewitt, M. (2021). A data dividend that works: steps toward building an equitable data economy.

Fisher, R. J. (1993). Social desirability bias and the validity of indirect questioning. *Journal of consumer research, 20*(2), 303-315.

Floridi, L. (2016). On human dignity as a foundation for the right to privacy. *Philosophy & Technology, 29*(4), 307-312.

Fordsham, N., Moss, A. J., Krumholtz, S., Roggina, T., Robinson, J., & Litman, L. (2019). Variation among Mechanical Turk Workers Across Time of Day Presents an Opportunity and a Challenge for Research.

Fox, J., & Moreland, J. J. (2015). The dark side of social networking sites: An exploration of the relational and psychological stressors associated with Facebook use and affordances. *Computers in Human Behavior, 45*, 168-176.

Fragale, A. R., Rosen, B., Xu, C., & Merideth, I. (2009). The higher they are, the harder they fall: The effects of wrongdoer status on observer punishment recommendations and intentionality attributions. *Organizational Behavior and Human Decision Processes, 108*(1), 53-65.

Fraiberger, S. P., & Sundararajan, A. (2017). Peer-to-peer rental markets in the sharing economy. *NYU Stern School of Business Research Paper (First version March 2015*.

Friggeri, A., Adamic, L., Eckles, D., & Cheng, J. (2014). *Rumor cascades.* Paper presented at the Proceedings of the International AAAI Conference on Web and Social Media.

Frischmann, B., & Selinger, E. (2018). *Re-engineering humanity*: Cambridge University Press.

Froomkin, M. (2015). *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*. University of Miami School of Law Institutional Repository.

Furnham, A. (1986). Response bias, social desirability and dissimulation. *Personality and individual differences, 7*(3), 385-400.

Gertsen, F., & Oosterlaken, I. (2018). *From Footprint to Mindprint; White Paper, Stevanovich Institute on the Formation of Knowledge*. Retrieved from The University of Chicago: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3479629

Ghorayshi, A., & Ray, S. (2018, April 2, 2018). Grindr Is Letting Other Companies See User HIV Status And Location Data. *BuzzFeed News*.

Gillespie, T. (2014). The relevance of algorithms. *Media technologies: Essays on communication, materiality, and society, 167*(2014), 167.

Goel, S., Anderson, A., Hofman, J., & Watts, D. J. (2016). The structural virality of online diffusion. *Management Science, 62*(1), 180-196.

Gold, Z., & Latonero, M. (2017). Robots Welcome: Ethical and Legal Considerations for Web Crawling and Scraping. *Wash. JL Tech. & Arts, 13*, 275.

Google Inc. Gmail Litigation, No. 5:13-md-02430-LHK (United States District Court: Northern District of California 2013).

Goulder, L. H. (1995). Environmental taxation and the double dividend: a reader's guide. *International Tax and Public Finance, 2*(2), 157-183.

Gross, C., Lorek, K., & Richter, F. (2017). Attitudes towards inheritance taxation–results from a survey experiment. *The Journal of Economic Inequality, 15*(1), 93-112.

Gruber, J., & Koszegi, B. (2002). *A theory of government regulation of addictive bads: optimal tax levels and tax incidence for cigarette excise taxation*. Retrieved from

Guadagno, R. E., Rempala, D. M., Murphy, S., & Okdie, B. M. (2013). What makes a video go viral? An analysis of emotional contagion and Internet memes. *Computers in Human Behavior, 29*(6), 2312-2319.

Guess, A., Nyhan, B., & Reifler, J. (2018). Selective exposure to misinformation: Evidence from the consumption of fake news during the 2016 US presidential campaign. *European Research Council, 9*.

Guler, S. (2019). *The Good, The Bad, and The Taxed: How Taxes Shape Morals in Markets.*

Hallinan, D., & De Hert, P. (2017). Genetic classes and genetic categories: protecting genetic groups through data protection law. In *Group Privacy* (pp. 175-196): Springer.

Hamari, J., Koivisto, J., & Pakkanen, T. (2014). *Do persuasive technologies persuade?-a review of empirical studies.* Paper presented at the International conference on persuasive technology.

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*, 21.

Hayes, A. F. (2018). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (Second ed.): Guilford publications.

Hirsch, D. D. (2006). Protecting the inner environment: What privacy regulation can learn from environmental law. *Ga. L. Rev., 41*, 1.

Hirsch, D. D., & King, J. H. (2016). Big Data Sustainability: An Environmental Management Systems Analogy. *Washington and Lee Law Review Online, 72*(3), 406.

Holland, G., & Tiggemann, M. (2016). A systematic review of the impact of the use of social networking sites on body image and disordered eating outcomes. *Body image, 17*, 100-110.

Hui, C., Tyshchuk, Y., Wallace, W. A., Magdon-Ismail, M., & Goldberg, M. (2012). *Information cascades in social media in response to a crisis: a preliminary model and a case study.* Paper presented at the Proceedings of the 21st International Conference on World Wide Web.

Humbert, M., Trubert, B., & Huguenin, K. (2019). A survey on interdependent privacy. *ACM Computing Surveys (CSUR), 52*(6), 1-40.

Ibrahim, Y. (2015). Instagramming life: Banal imaging and the poetics of the everyday. *Journal of Media Practice, 16*(1), 42-54.

Jacobs, B., & De Mooij, R. A. (2015). Pigou meets Mirrlees: On the irrelevance of tax distortions for the second-best Pigouvian tax. *Journal of Environmental Economics and Management, 71*, 90-108.

Jalili, M., & Perc, M. (2017). Information cascades in complex networks. *Journal of Complex Networks, 5*(5), 665-693.

Jin, G. Z. (2019). 18. Artificial Intelligence and Consumer Privacy. In A. Agrawal, J. S. Gans, & A. Goldfarb (Eds.), *The Economics of Artificial Intelligence* (pp. 439-492): University of Chicago Press.

Jinyan Zang, K. D., James Graves, Paul Lisker, Latanya Sweeney. (2015). Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps. *Technology Science*. Retrieved from https://techscience.org/a/2015103001/

Käß, S., Schnürer, S., & Miller, M. (2021). Social Media and the Realms of Addictive Behavior.

Kool, L., Timmer, J., Royakkers, L., & Est van, R. (2017). *Urgent Upgrade: Protect Public Values in our Digitized Society*. Retrieved from The Hague: https://www.rathenau.nl/en/digitale-samenleving/urgent-upgrade

Kool, L., Timmer, J., Royakkers, L., & van Est, Q. (2017). Urgent upgrade: protect public values in our digitized society.

Köthenbürger, M. (2020). *Taxation of Digital Platforms*. Retrieved from

Krol, K., & Preibusch, S. (2016). *Control versus effort in privacy warnings for webforms.* Paper presented at the Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society.

Kroll, H., Horvat, D., & Jäger, A. (2018). *Effects of automatisation and digitalisation on manufacturing companies' production efficiency and innovation performance*. Retrieved from

Laaksonen, S.-M., Haapoja, J., Kinnunen, T., Nelimarkka, M., & Pöyhtäri, R. (2020). The datafication of hate: expectations and challenges in automated hate speech monitoring. *Frontiers in big Data, 3*, 3.

Lammi, M., & Pantzar, M. (2019). The data economy: How technological change has altered the role of the citizen-consumer. *Technology in Society, 59*, 101157.

Landau, S. (2013). Making sense from Snowden: What's significant in the NSA surveillance revelations. *IEEE Security & Privacy, 11*(4), 54-63.

Lavorgna, A. (2021). *Information Pollution as Social Harm: Investigating the Digital Drift of Medical Misinformation in a Time of Crisis*: Emerald Group Publishing.

Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., . . . Rothschild, D. (2018). The science of fake news. *Science, 359*(6380), 1094-1096.

Lee, Z. W., Cheung, C. M., & Chan, T. K. (2021). Understanding massively multiplayer online role-playing game addiction: A hedonic management perspective. *Information Systems Journal, 31*(1), 33-61.

Li, H., Zhu, H., Du, S., Liang, X., & Shen, X. (2016). Privacy leakage of location sharing in mobile social networks: Attacks and defense. *IEEE Transactions on Dependable and Secure Computing, 15*(4), 646-660.

Lindquist, B., & Hermansson, P. (Writers) & H. N. Hate (Director). (2018). Undercover in the Alt-Right. In. UK.

Litman, L., & Robinson, J. (2020). *Conducting Online Research on Amazon Mechanical Turk and Beyond*: Sage Publications.

Lorenzi, P. (2004). Sin taxes. *SOCIETY-NEW BRUNSWICK-, 41*(3), 59-65.

MacCarthy, M. (2010). New directions in privacy: Disclosure, unfairness and externalities. *ISJLP, 6*, 425.

Maldoff, G., & Tene, O. (2019). The Costs of Not Using Data: Balancing Privacy and the Perils of Inaction. *Journal of Law, Economics and Policy, 15*(1), 41.

Malik, A., Dhir, A., & Nieminen, M. (2016). Uses and gratifications of digital photo sharing on Facebook. *Telematics and Informatics, 33*(1), 129-138.

Marian, O. Y. (2021). Taxing Data. *UC Irvine School of Law Research Paper*(2021-17).

Mason, W., & Suri, S. (2012). Conducting behavioral research on Amazon's Mechanical Turk. *Behavior research methods, 44*(1), 1-23.

Masud, S., Dutta, S., Makkar, S., Jain, C., Goyal, V., Das, A., & Chakraborty, T. (2021). *Hate is the New Infodemic: A Topic-aware Modeling of Hate Speech Diffusion on Twitter.* Paper presented at the 2021 IEEE 37th International Conference on Data Engineering (ICDE).

Mathew, B., Dutt, R., Goyal, P., & Mukherjee, A. (2019). *Spread of hate speech in online social media.* Paper presented at the Proceedings of the 10th ACM conference on web science.

McFarland, S. G. (1981). Effects of question order on survey responses. *Public opinion quarterly, 45*(2), 208-215.

Meel, P., & Vishwakarma, D. K. (2020). Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities. *Expert Systems with Applications, 153*, 112986.

Mejias, U. A., & Couldry, N. (2019). Datafication. *Internet Policy Review, 8*(4).

Metcalf, G. E., & Weisbach, D. (2009). The design of a carbon tax. *Harv. Envtl. L. Rev., 33*, 499.

Mian, A., & Khan, S. (2020). Coronavirus: the spread of misinformation. *BMC medicine, 18*(1), 1-2.

Mingers, J. C. (1995). Information and meaning: foundations for an intersubjective account. *Information Systems Journal, 5*(4), 285-306.

Mizrahi, S. (2020). Cascading disasters, information cascades and continuous time models of domino effects. *International journal of disaster risk reduction, 49*, 101672.

Morgan, S. (2020). The World Will Store 200 Zettabytes of Data by 2025. *Cybercrime Magazine*.

Murphy, A. (2017). Dating dangerously: risks lurking within mobile dating apps. *Cath. UJL & Tech, 26*, 100.

Myovella, G., Karacuka, M., & Haucap, J. (2020). Digitalization and economic growth: A comparative analysis of Sub-Saharan Africa and OECD economies. *Telecommunications Policy, 44*(2), 101856.

Myrstad, F., & Tjøstheim, I. (2021). Out of Control. How consumers are exploited by the online advertising industry.

Nielsen, J. (2003, November 2003). "IM, Not IP (Information Pollution)". *ACM Queue, 1(8),* 75-76.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs, 41*(1), 100-126.

Nussbaum, M. C. (2011). *Creating Capabilities: The Human Development Approach*. Cambridge: The Belknap Press of Harvard University Press.

O'Donoghue, T., & Rabin, M. (2006). Optimal sin taxes. *Journal of Public Economics, 90*(10-11), 1825-1849.

OECD. (2019). *How's Life in the Digital Age; Opportunities and Risks of the Digital Transformation for People's Well-Being*. Retrieved from Paris:

Olejnik, L., Kutrowska, A., & Castelluccia, C. (2014). *The beginning of genetic exhibitionism?* Paper presented at the Proceedings of the 1st Workshop on Genome Privacy.

Ostheimer, J., & Iqbal, S. (2019). *Privacy in online dating: does it matter?* Paper presented at the Proceedings of the 3rd International Conference on Cryptography, Security and Privacy.

Özdemir, Ş. (2016). Individual contributions to infollution (information pollution): trust and share. *International Journal on New Trends in Education and Their Implications, 7*(2), 23-33.

Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running experiments on amazon mechanical turk. *Judgment and Decision making, 5*(5), 411-419.

Park, S., Sang, Y., Jung, J., & Stroud, N. J. (2021). News Engagement: The Roles of Technological Affordance, Emotion, and Social Endorsement. *Digital journalism, 9*(8), 1007-1017.

Park, Y. (2021). *The Future of Digital Surveillance: Why Digital Monitoring Will Never Lose Its Appeal in a World of Algorithm-driven AI*: University of Michigan Press.

Pearce, W., Özkula, S. M., Greene, A. K., Teeling, L., Bansard, J. S., Omena, J. J., & Rabello, E. T. (2020). Visual cross-platform analysis: Digital methods to research social media images. *Information, Communication & Society, 23*(2), 161-180.

Perloff, R. M. (1999). The third person effect: A critical review and synthesis. *Media psychology, 1*(4), 353-378.

Phillips, W. (2019). It wasn't just the trolls: Early internet culture,"fun," and the fires of exclusionary laughter. *Social Media+ Society, 5*(3), 2056305119849493.

Phillips, W., & Milner, R. M. (2021). *You are here: A field guide for navigating polarized speech, conspiracy theories, and our polluted media landscape*: MIT Press.

Pierri, F., Piccardi, C., & Ceri, S. (2020). Topology comparison of Twitter diffusion networks effectively reveals misleading information. *Scientific reports, 10*(1), 1-9.

Pigou, A. C. (2013). *The Economics of Welfare* (Fourth ed.). London: Palgrave Macmillan.

Preibusch, S., Krol, K., & Beresford, A. R. (2013). The privacy economics of voluntary over-disclosure in Web forms. In *The Economics of Information Security and Privacy* (pp. 183-209): Springer.

Qualtrix. (2020). Provo, Utah. Retrieved from https://www.qualtrics.com/blog/citing-qualtrics/

Reed, W. R. (2006). Democrats, republicans, and taxes: Evidence that political parties matter. *Journal of Public Economics, 90*(4-5), 725-750.

Richards, N., & Hartzog, W. (2016). Privacy's Trust Gap: A Review. *Yale lJ, 126*, 1180.

Richards, N. M. (2012). The dangers of surveillance. *Harv. L. Rev., 126*, 1934.

Richards, N. M., & Hartzog, W. (2020). Privacy's Constitutional Moment. *Boston College Law Review*(61), 79.

Rivers, D. J. (2020). Strava as a discursive field of practice: Technological affordances and mediated cycling motivations. *Discourse, Context & Media, 34*, 100345.

Robinson, J., Rosenzweig, C., Moss, A. J., & Litman, L. (2019). Tapped out or barely tapped? Recommendations for how to harness the vast and largely unused potential of the Mechanical Turk participant pool. *PLoS one, 14*(12), 1 - 29. Retrieved from https://doi.org/10.1371/journal.pone.0226394

Romer, P. (2021) *Why We Should Tax Digital Advertising/Interviewer: L. Zingales*. Capital Isn't, University of Chicago.

Rowe, F., Ngwenyama, O., & Richet, J.-L. (2020). Contact-tracing apps and alienation in the age of COVID-19. *European journal of information systems, 29*(5), 545-562.

Royakkers, L., Timmer, J., Kool, L., & van Est, R. (2018). Societal and ethical issues of digitization. *Ethics and Information Technology, 20*(2), 127-142.

Rushe, D. (2013, August 15, 2013). Google: don't expect privacy when sending to Gmail. *The Guardian*.

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American psychologist, 55*(1), 68.

Sanchez-Cartas, J. M. (2020). Intellectual property and taxation of digital platforms. *Journal of Economics*, 1-25.

Sanderson, Z., Brown, M. A., Bonneau, R., Nagler, J., & Tucker, J. A. (2021). Twitter flagged Donald Trump's tweets with election misinformation: They continued to spread both on and off the platform. *Harvard Kennedy School Misinformation Review*.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*: WW Norton & Company.

Schoeman, F. D. (1992). *Privacy and social freedom*: Cambridge university press.

Schudy, S., & Utikal, V. (2017). 'You must not know about me'—On the willingness to share personal data. *Journal of Economic Behavior & Organization, 141*, 1-13.

Schwartz, P. M., & Peifer, K.-N. (2017). Transatlantic Data Privacy Law. *Geo. LJ, 106*, 115.

Sen, A. (2001). *Development as freedom*: Oxford Paperbacks.

Sharma, S. (2013). Black Twitter? Racial hashtags, networks and contagion. *New Formations, 78*(78), 46-64.

Sharma, T., & Bashir, M. (2020). Use of apps in the COVID-19 response and the loss of privacy protection. *Nature Medicine, 26*(8), 1165-1167.

Shaw, F. (2016). "Bitch I said hi": The Bye Felipe campaign and discursive activism in mobile dating apps. *Social Media+ Society, 2*(4), 2056305116672889.

Simpson, R. M. (2013). Dignity, harm, and hate speech. *Law and Philosophy, 32*(6), 701-728.

Skaza, J., & Blais, B. (2017). Modeling the infectiousness of Twitter hashtags. *Physica A: Statistical Mechanics and its Applications, 465*, 289-296.

Slater, M. D. (2007). Reinforcing spirals: The mutual influence of media selectivity and media effects and their impact on individual behavior and social identity. *Communication theory, 17*(3), 281-303.

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age* (Vol. 1): NyU Press.

Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev., 126*, 1880.

Solove, D. J., & Citron, D. K. (2017). Risk and anxiety: A theory of data-breach harms. *Tex. L. Rev., 96*, 737.

Solow-Niederman, A. (2021). Information Privacy and the Inference Economy. *Available at SSRN 3921003*.

Springer, A. L. (1977). Towards a meaningful concept of pollution in international law. *International & Comparative Law Quarterly, 26*(3), 531-557.

Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. *Internet Policy Review, 8*(2).

Sutherland, W., & Jarrahi, M. H. (2018). The sharing economy and digital platforms: A review and research agenda. *International Journal of Information Management, 43*, 328-341.

Tasnim, S., Hossain, M. M., & Mazumder, H. (2020). Impact of rumors or misinformation on coronavirus disease (COVID-19) in social media.

Tau, B. (2020, June 19, 2020). IRS Used Cellphone Location Data to Try to Find Suspects. *Wall Street Journal*.

Tau, B., & Hackman, M. (2020, February 7, 2020). Federal Agencies Use Cellphone Location Data for Immigration Enforcement. *Wall Street Journal*.

Taylor, L., Floridi, L., & Van der Sloot, B. (2016). *Group privacy: New challenges of data technologies* (Vol. 126): Springer.

Thimmesch, A. B. (2016). Transacting in Data: Tax, Privacy, and the New Economy.

Thomson, S. A., & Warzel, C. (2019, December 19, 2019). One Nation, Tracked: An Investigation Into the Smartphone Tracking Industry From Times Opinion. *N.Y. Times*. Retrieved from https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

Tietenberg, T., & Lewis, L. (2018). *Environmental and natural resource economics*: Routledge.

Tiggemann, M., Hayden, S., Brown, Z., & Veldhuis, J. (2018). The effect of Instagram "likes" on women's social comparison and body dissatisfaction. *Body image, 26*, 90-97.

Trepte, S. (2020). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication theory*.

Tucker, C. (2019). 17. Privacy, Algorithms, and Artificial Intelligence. In *The Economics of Artificial Intelligence* (pp. 423-438): University of Chicago Press.

Turrini, M. (2018). Online genomes: problematizing the disruptiveness of direct-to-consumer genetic tests. *Sociology Compass, 12*(11), e12633.

Twenge, J. M., Haidt, J., Blake, A. B., McAllister, C., Lemon, H., & Le Roy, A. (2021). Worldwide increases in adolescent loneliness. *Journal of Adolescence*.

Van Ark, B. (2015). Productivity and digitilization in Europe: Paving the road to faster growth. *Digiworld Economic Journal*(100), 107.

Van Kleek, M., Liccardi, I., Binns, R., Zhao, J., Weitzner, D. J., & Shadbolt, N. (2017). *Better the devil you know: Exposing the data sharing practices of smartphone apps.* Paper presented at the Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems.

Vishwanath, A. (2016). Mobile device affordance: Explicating how smartphones influence the outcome of phishing attacks. *Computers in Human Behavior, 63*, 198-207.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146-1151.

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Colum. Bus. L. Rev.*, 494.

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making*. Retrieved from Strasbourg:

Warner, M., Gutmann, A., Sasse, M. A., & Blandford, A. (2018). Privacy unraveling around explicit HIV status disclosure fields in the online geosocial hookup app Grindr. *Proceedings of the ACM on Human-Computer Interaction, 2*(CSCW), 1-22.

West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society, 58*(1), 20-41.

Whelan, E., & Clohessy, T. (2020). How the social dimension of fitness apps can enhance and undermine wellbeing: A dual model of passion perspective. *Information Technology & People*.

Wilson, K. (2017). Does public competition crowd out private investment? Evidence from municipal provision of internet access. *Evidence from Municipal Provision of Internet Access (June 16, 2017) .NET Institute Working Paper*(16-16).

Withagen, R., De Poel, H. J., Araújo, D., & Pepping, G.-J. (2012). Affordances can invite behavior: Reconsidering the relationship between affordances and agency. *New Ideas in Psychology, 30*(2), 250-258.

Yim, D., Malefyt, T., & Khuntia, J. (2021). Is a picture worth a thousand views? Measuring the effects of travel photos on user engagement using deep learning algorithms. *Electronic markets*, 1-19.

Zannettou, S., Finkelstein, J., Bradlyn, B., & Blackburn, J. (2020). *A quantitative approach to understanding online antisemitism.* Paper presented at the Proceedings of the International AAAI Conference on Web and Social Media.

Zell, E., Strickhouser, J. E., Sedikides, C., & Alicke, M. D. (2020). The better-than-average effect in comparative self-evaluation: A comprehensive review and meta-analysis. *Psychological Bulletin, 146*(2), 118.

Zhou, X., & Rau, P.-L. P. (2021). *Valuing Social Media Affordances.* Paper presented at the International Conference on Human-Computer Interaction.

Zingales, L. R., Guy; Lancieri, Filippo. (2019). *Stigler Committee on Digital Platforms - Final Report*. Retrieved from The University of Chicago: https://research.chicagobooth.edu/stigler/media/news/committee-on-digital-platforms-final-report

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75-89.

Zuboff, S. (2019a). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*: Profile Books.

Zuboff, S. (2019b). *Surveillance capitalism and the challenge of collective action.* Paper presented at the New labor forum.

*****