WORKING PAPER

Privacy Paradox – Economic Uncertainty Theory and Legal Consequences

by

Sarah Geschonke and Thomas Wein

University of Lüneburg
Working Paper Series in Economics

No. 393

August 2020

www.leuphana.de/institute/ivwl/forschung/working-papers.html

ISSN 1860 - 5508

Privacy Paradox –

Economic Uncertainty Theory and Legal Consequences

Sarah Geschonke

Thomas Wein

Aug-20

Planned to be submitted to “European Journal of Law and Economics”

Corresponding Author:

Prof. Dr. Thomas Wein
Institute of Economics
Competition and Regulation Institute
Leuphana University of Lüneburg
Universitätsallee 1
D-21335 Lüneburg
Germany
++49/4131/6772302 (phone)
++49/4131/6772026 (fax)
wein@leuphana.de
https://www.leuphana.de/institute/cri/personen/thomas-wein.html

Abstract

Internet users generously disclose personal information to consume supposedly "free" digital services despite severe privacy concerns—a phenomenon termed privacy paradox. Humanities have thoroughly studied this discrepancy in attitude and behavior, yet have not developed a conclusive explanation for its occurrence, let alone a means to counter it. Both the quantity and the quality of data privacy laws, as well as the increasing number of court rulings dealing with digital business models, show the urgent need to better understand the cause of the privacy paradox and to mitigate it. This paper analyzes the contradictory phenomenon from an economic point of view. By applying the two-state of the world-model, the authors demonstrate that uncertainty about the extent and the likelihood of a data breach are explanatory factors for the privacy paradox. Taking the European General Data Protection Regulation as an exemplary showcase, the authors further examine the role of privacy laws to offset Internet users' inconsistent privacy behavior. In theory, such a "rights and remedies" scheme is intended to counter the uncertainty factors provoking the privacy paradox; however, in practice, this intention is only partially served.

JEL-Classification: K24, L15, L86

Key words: Data protection, Privacy paradox, Legal remedies

Individuals can be quite self-contradictory when it comes to their private sphere. In 2019, three out of four global citizens have been at least somewhat concerned about their digital privacy.[1] Nevertheless, that same year, global online users posted almost 278,000 Instagram stories, swiped 1.4 million potential Tinder dates, and conducted almost 4.5 million Google searches—and those were the statistics for only one minute of internet time.[2] Notwithstanding the serious concerns about the loss of control over personal data, digital users ("data subjects") disclose their information rather generously. This inconsistency in attitude and behavior has been termed the "privacy paradox."[3]

Scholars, especially of the social and psychological sciences, have diligently been approaching this phenomenon with a variety of theoretical lenses to shed light on both its cause as well as potential means to counter it.[4] So far, however, there are no conclusive answers to the question of why privacy-sensitive individuals would barter their personal information for the consumption of online services instead of paying a regular price, and thereby preserving their privacy.

Current developments in both the quality and the quantity of privacy legislations and jurisdictions demonstrate that the urge to solve the privacy paradox has moved well beyond scholarly debate. The rapidly increasing number of privacy laws around the globe,[5] as well as novel legal rights and remedy schemes—as exemplified by the European General Data

[1] Ipsos, 8.

[2] Domo.

[3] Brown, B.; Norberg, Horne, and Horne; Barnes.

[4] For comprehensive literature reviews on privacy paradox that includes economic, psychological and social science-based approaches, see Kokolakis; Barth and Jong; Gerber, Gerber, and Volkamer.

[5] Greenleaf.

Protection Regulation ("GDPR")[6] as the contemporary flagship of privacy law—are strong indicators of the importance of this issue. As well, recent decisions dealing with the sharing, processing, and monetization of online users' personal data, in regard to social media services[7] and online gambling,[8] underline the need to further investigate the cause of the privacy paradox.

This paper aims to contribute to the investigation of the paradoxical privacy behavior of data subjects with a novel economic analysis. While the majority of economic research has to this point primarily focused on behavioral economics to explain the rationale of the phenomenon,[9] the authors of this paper go one step further. By applying the two-state-of the world-model[10], the article examines factors of uncertainty that provoke contradictory privacy behavior.

In economic terms, the privacy paradox constitutes a market failure. Therefore, a regulatory intervention in the market by the means of data privacy law would be justified. In theory, data protection law intends to mitigate this equivocal privacy behavior, yet the actual effectiveness of the law is questionable. Therefore, the authors further analyze the impact of the novel GDPR on factors of uncertainty that contribute to the privacy paradox.

This paper is structured as follows. First, it briefly delineates the phenomenon of the privacy paradox. Second, the article examines the root of this paradox by applying the two-state-framework of uncertainty as an argument for insufficient data protection demand. Third, the

[6] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L [2016] 119/1.

[7] See, e.g. Oberlandesgericht Düsseldorf, Facebook; European Court of Justice, Fashion ID.

[8] See, e.g. Oberlandesgericht Frankfurt, Gewinnspiel; European Court of Justice, Planet49.

[9] Acquisti; Acquisti and Grossklags, "Privacy and rationality".

[10] Cullis and Jones, 244–46.

paper discusses the role of data protection regulation, i.e. the GDPR, to conciliate the discrepancy between privacy attitude and behavior. The final paragraph concludes with legal and economic consequences.

The Privacy Paradox

Along with the increasing commercialization of the Internet since 1995, scholars have detected a discrepancy between consumers' privacy attitude and their privacy behavior. Despite lamenting serious concerns about the loss of control over their personal information[11] on the Internet, data subjects continue to unconsciously generate and consciously self-disclose personal data on a large scale: a phenomenon termed the "privacy paradox."[12]

The prevalence of this contradictory privacy behavior has frequently been investigated in social sciences and psychology. The majority of this research has corroborated the discrepancy between privacy attitude and actual data-disclosing behavior.[13] The privacy paradox has in fact been verified in different realms of the online world, e.g. in the use of smart devices[14], e-commerce,[15] online banking,[16] and particularly in social media services[17]. Hence, online users

[11] In this context, personal data comprise any information relating to an identified or identifiable natural person, such as voluntarily provided data, observable traffic data, and inferred data. For an in-depth explanation of the different types of data, see OECD; also Jentzsch.

[12] Brown, B.; Norberg, Horne, and Horne; Barnes.

[13] Relatively few studies partly refute the privacy paradox, see, e.g. D'Souza and Phelps; Boyles, Smith, and Madden; Dienlin and Trepte; Baek; Heravi, Mubarak, and Raymond Choo; Gruzd and Hernández-García.

[14] Williams, Nurse, and Creese.

[15] Spiekermann, Grossklags, and Berendt; Berendt, Günther, and Spiekermann; Beresford, Kübler, and Preibusch.

[16] Nofer et al.

[17] Acquisti and Gross; Tufekci; Reynolds et al.; Taddicken; Young and Quan-Haase; Chen and Cheung.

use their personal data as indirect "currency" instead of paying a direct monetary fee to consume digital services.

The processing and monetization of consumer data has increasingly spurred significant developments in global privacy legislations. First of all, the amount of global privacy laws have significantly increased in the past decade. By 2019, almost 70 percent of countries around the globe have had privacy jurisdictions in place for both the public and the private sector, or at least have had respective bills in progress.[18] Secondly, the quality of both newly enacted and revised data protection legislation adjusts to the dynamics of the digital market. In this regard, the novel protection scheme of the GDPR is often used as a blueprint (compare to the "The Privacy Paradox and the General Data Protection Regulation" section).[19]

As well, jurisprudence increasingly engages in cases dealing with the processing of data that online users consent to disclose in order to consume seemingly "free" digital services. The following examples of contemporary case law in the EU and Germany demonstrate this trend:

a) In February 2019, the German Federal Cartel Office accused Facebook as being the world's largest social network to exploitatively abuse its dominant market position to gather information about data subjects without their consent.[20] In detail, the anti-trust authority reprimanded Facebook for collecting data from third-party apps, including its own Instagram and WhatsApp, as well as tracking online users who are not members through Facebook "like" or "share" buttons. Against this backdrop, the cartel office prohibited the dissemination of data and ordered Facebook to change its terms and conditions within a year. In August 2019, however, the relevant Düsseldorf Higher

[18] Greenleaf.

[19] Ibid.

[20] Bundeskartellamt, Facebook.

Regional Court suspended this landmark decision because of serious doubts about its legality.[21] In fact, the court did not find data subjects who autonomously and consciously consented to disclose their information to have been abusively exploited.

b) In July 2019, the Court of Justice of the European Union ("CJEU") also delivered a judgment in regard to the embedded Facebook "Like" button on a third-party website, namely the online shop of the retailer Fashion ID.[22] In this case, a German consumer protection association brought an action asserting that the retailer's use of the "Like" plug-in breached EU-data protection legislation. In detail, the association accused Fashion ID of neither providing appropriate notice about the extensive and primarily covert data processing taking place through the social plug-in, nor collecting consent for it.[23] Building on the two previous judgments of joint data controllership,[24] the highest EU court partially endorsed the association's standpoint and found the retailer responsible for the initial collection and secondary transmission of personal data to Facebook. The court did not, however, find the retailer responsible for the subsequent data processing done by Facebook itself. As a result of the decision, website operators that implement social media plug-ins are required to inform their users about the data transfer and to obtain required consent.

[21] Oberlandesgericht Düsseldorf, Facebook.

[22] European Court of Justice, Fashion ID.

[23] In fact, by having implemented the "like"-button on its website, the retailer automatically shared data subjects' IP addresses and browser strings with Facebook without the data subjects being aware of this data disclosure. Moreover, this data transmission took place regardless of whether the data subjects actually clicked on the button or had a Facebook account.

[24] European Court of Justice, Wirtschaftsakademie Schleswig-Holstein; Jehovan Todistajat.

c) In June 2019, the Higher Regional Court of Frankfurt am Main ("OLG Frankfurt") also dealt with data subjects' consent in the digital context, regarding online gambling.[25] The court took a comparatively lenient stance, in contrast to the commonly rather restrictive German interpretation of data protection standards in general, and of the concept of "voluntary consent" in particular. First, the OLG Frankfurt ruled that participation in an online raffle can be made dependent on data subjects' consent to receive future advertising, including promotions via e-mail or telephone from several different third-party advertising companies. With this coupling incentivization, the court shifted the responsibility to the consumers, who are held accountable to decide for themselves if online gambling is "worth" the disclosure of their personal information.

d) In October 2019, the European Court of Justice dealt with another online gambling case, which the German Federal Court of Justice referred to them. This time, the CJEU assessed the cookie transparency and consent requirements for an online promotional lottery offered by the company Planet49.[26] The Federation of German Consumer Organizations (Verbraucherzentrale Bundesverband) took legal action against the company claiming that the required declaration of consent did not meet German data protection standards. In detail, data subjects interested in participating in the digital sweepstakes were presented two checkboxes: one unticked consent-checkbox for advertising purposes, which was mandatory for the participation in the lottery, and another pre-ticked consent-checkbox for cookies. The court primarily focused on the legitimacy of the second checkbox and held that consent obtained through pre-ticked cookie-checkboxes would not be valid ("opt-out" practice). Therefore, cookies used for

[25] Oberlandesgericht Frankfurt, Gewinnspiel.

[26] European Court of Justice, Planet49.

> marketing purposes require actively given confirmation from the user—regardless of whether the cookies collected personal information or merely tracked browsing habits. Moreover, the court declared data processors must be responsible for informing users about both the duration of time the cookie information would be kept, as well as disclosing third party access to the data. This action would enable users to make informed decisions when providing their personal information online.[27]

In summary, although individuals could choose to participate in fee-based online gambling lotteries or social media networks that protect their data, a significant share of them nevertheless decides to barter away their privacy. The recent examples of privacy case law illustrate the indecisiveness of how to interpret data subjects' paradoxical privacy behavior, as well as legal ramifications when users—more or less willingly—consent to reveal their personal data. The courts interpreted the role of the data subjects very differently; in some cases, courts appealed to users' self-responsibility, and in others, the judgments entailed comprehensive consumer protection.

Given these significant implications of the privacy paradox for the society, the economy, and the legal system, scholars have been focusing their research on factors that contribute to this paradoxical phenomenon.

A starting point for understanding the cause of the privacy paradox from an economic point of view constitutes the "privacy calculus model."[28] According to this model, rational agents weigh

[27] This judgment had not directly translated into German law, because Germany had not fully implemented the European-Privacy Directive (popularly known as "Cookie Directive"). However, largely building on the CJEU's Planet49 decision, the German Federal Court of Justice ruled on requirements that must be met to obtain valid cookie consent in May 2020. See Bundesgerichtshof, Cookie-Einwilligung II.

[28] Culnan and Armstrong.

perceived costs against perceived benefits in their decision-making process. Adjusting the privacy cost-benefit trade-off to the digital world, data subjects weigh expected losses of privacy against potential gains of disclosing personal data in their privacy assessment. They are willing to disclose their data to a website, an app or a smart device, if the perceived benefits outweigh the perceived tangible and intangible costs.[29] Building on this idea, a growing body of literature refined the neoclassical privacy calculus model to better explain the privacy paradox in reality by adapting two key propositions.

First, scholars argued that the disclosure of personal information is a highly contextual decision.[30] Accordingly, data subjects' assessment of their perceived costs and benefits of data disclosure can be dependent on very situation-specific factors.[31] Scholars have thus extended the privacy calculus model to include contextual factors, such as, data subjects' perceived trust in the data controllers and processors ("data holders") or perceived risk of data disclosure,

[29] Hann et al.; Chellappa and Sin; Keith et al.; Knijnenburg, Kobsa, and Jin; Jiang, Heng, and Choi; Gimpel, Kleindienst, and Waldmann.

[30] John, Acquisti, and Loewenstein; Acquisti, John, and Loewenstein.

[31] Scholars have for instance identified an impact of the social environment and resultant social needs on data subjects' privacy assessment, see, e.g. Ellison et al.; Taddicken; Lee, Park, and Kim; Buck et al.; Debatin et al.; Hew et al. Also, the cultural environment can influence the privacy behavior, see, e.g. Miltgen and Peyrat-Guillard; Dinev et al. Besides, contextual valuation for different

types of data, e.g. browsing history, health data, or other sensitive data, can affect the privacy assessment, see, e.g. Carrascal et al.; Huberman, Adar, and Fine; Mothersbaugh et al. Moreover, scholars argue that a 'privacy cyncisms' can impact data disclosure, see, e.g. Hargittai and Marwick; Hoffmann, Lutz, and Ranzini; Shklovski et al.

among other things.[32] As such, situation-specific conditions may overrule pre-existing privacy attitudes, and can constitute a cause of the privacy paradox.

Second, scholars, most notably behavioral economists, propose data subjects' bounded rationality as an explanatory factor for their paradoxical privacy behavior. Thus, Internet users cannot absorb and process relevant information about data processing, data protection, and potential privacy violations because of both limited cognitive capabilities[33] and resources[34]. This bounded rationality creates an information asymmetry to the detriment of data subjects. As a result, data subjects base their data privacy assessment on cognitive heuristics,[35] which in turn result in privacy biases. For instance, overconfidence of personal privacy skills or an underestimation of the current or future privacy risk.[36] These deviations from rationality can also be an explanation for the privacy paradox.

The authors suggest that there could be another explanatory factor for the privacy paradox: uncertainty. Internet users can assess neither the probability nor the extent of a potential privacy infringement. Because of this ignorance—or rather this uncertainty—Internet users' privacy behavior does not align with their privacy attitude.

---

[32] Dinev and Hart; Anderson and Agarwal; Xu et al.; Li, Sarathy, and Xu; Kehr, Wentzel, and Kowatsch; Kehr, Wentzel, and Mayer; Dienlin and Metzger; Pentina et al.; Chen

[33] Acquisti; Acquisti and Grossklags, "Privacy and rationality"; Hoofnagle et al.; Hoofnagle and Urban; McDonald and Cranor, "Beliefs and Behaviors"; Kehr et al.; Wilson and Valacich; Bashir et al.

[34] McDonald and Cranor, "The Cost of Reading Privacy Policies".

[35] Sundar et al.; Gambino et al.; Kehr, Wentzel, and Mayer; Wakefield; Kehr, Wentzel, and Kowatsch.

[36] Baek, Kim, and Bae; Cho, Lee, and Chung; Acquisti and Grossklags, "Privacy Attitudes"; Wilson and Valacich; Acquisti; Brandimarte, Acquisti, and Loewenstein; Jensen, Potts, and Jensen; Acquisti and Grossklags, "Privacy and rationality"; Debatin et al.

The Privacy Paradox and Uncertainty

The uncertainty of privacy violation can be analyzed within a two-state-of the world-model.[37] *Figure 1* illustrates the effects of data infringement on a household's privacy. Our household has an exogenous starting income Y. Assuming the privacy of data subjects was intact, exogenous income would remain unchanged, which can be expressed by $Y^P(=Y)$. An infringement of privacy would reduce the income to Y^{NP}.

Assuming that *neither a statutory nor a contractual data protection scheme* between data subjects and data holders exist, the income in case of intact privacy can be written as privacy Y_0^P, equivalent to Y_0. A violation of privacy due to a data breach can be measured as income loss L. Thus, in case of a privacy infringement, the income would decrease to Y_0^{NP}, $Y_0 - L$. The probability of such a violation can be expressed by π, while the probability of unharmed privacy would be equivalent to $1 - \pi$; $0 < \pi < 1$.

Hence, expected income Y^e can be written as:

$$Y^e = \pi(Y_0 - L) + (1 - \pi)(Y_0) = Y_0 - \pi L.$$

The utilities of certain incomes are $U(Y)$ and $U(Y - L)$. The expected utility of privacy that is not subject to *statutory or contractual data protection* can be expressed by:

$$V(Y_0, Y_0 - L, \pi) = \pi U(Y_{NP}) + (1 - \pi)U(Y_0).$$

[37] Cullis and Jones, 244–46.

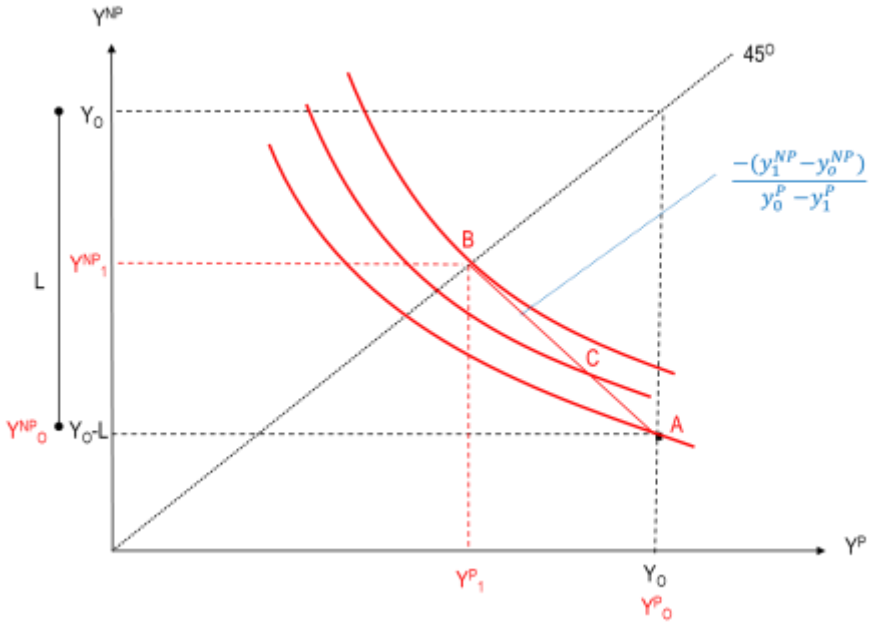

Figure 1: Privacy and Privacy Infringement

Figure 2 illustrates a household's risk aversion toward privacy infringements and its willingness to pay for data protection. Assuming the typical risk preferences of households ($U' > 0, U'' < 0$), 0.5 probabilities are expected for both states.

The willingness to pay for effective privacy protection in case of a data violation can be derived from the indifference curve V_0 by starting at point A and asking the individual data subject how much income she would be willing to give up for her personal data to be protected. Assuming the quality of the data protection increases gradually by the same amount (identical vertical distances), the willingness to pay for enhanced data protection decreases ($WTP_3 < WTP_2 < WTP_1$). Furthermore, the data subject has a lower willingness to a pay a risk premium, if the actual risk of a data breach decreases. This is illustrated by the slope of the indifference curve V_0 above the intercept with the certainty line (45°-line).

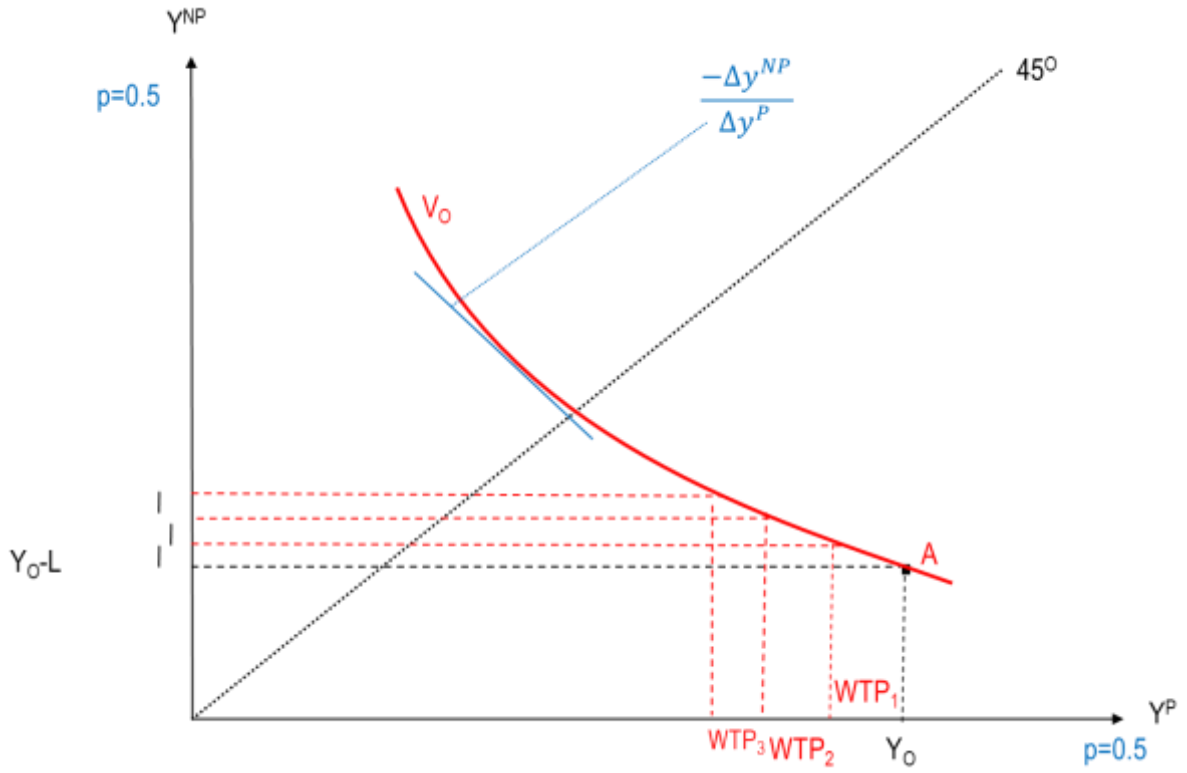

Figure 2: Risk Aversion and Willingness to pay

The expected utility remains constant along the indifference curve V_0,

$$dV = 0$$

$$\Rightarrow \pi \frac{\partial U(Y^{NP})}{\partial Y^{NP}} \Delta Y^{NP} + (1-\pi) \frac{\partial U(Y_o)}{\partial Y^P} \Delta Y^P = 0$$

$$\Rightarrow -\frac{(1-\pi)}{\pi} \frac{\frac{\partial U(Y_0)}{\partial Y^P}}{\frac{\partial U(Y^{NP})}{\partial Y^{NP}}} = \frac{\Delta Y^{NP}}{\Delta Y^P}.$$

Choosing a point on the indifference curve V_0 above the intercept with the 45°-line implies $Y^{NP} = Y^P$, which can be expressed by:

$$\frac{\partial U(Y_0)}{\partial Y^P} = \frac{\partial U(Y^{NP})}{\partial Y^{NP}}.$$

The slope of the tangent, i.e. the marginal rate of substitution of the indifference curve V_0 above the intercept with the 45°-line, therefore equals:

$$-\frac{(1-\pi)}{\pi} = \frac{\Delta Y^{NP}}{\Delta Y^{P}}.$$

In case of a *contractual data protection scheme,* data breaches might still occur, but the data holder would be required to compensate the data subject for incurred privacy losses (indemnity I). The respective losses are compensated according the compensation ratio q with $0 < q \leq 1$. If all losses were compensated $(q = 1)$, income would not vary with or without the privacy infringement (45°-line, point B in Figure *1*). The indemnity function can thus be written as:

$$I = qL.$$

Data holders offering *contractual data protection* can charge a proportional risk premium τ for their services. This supply of data protection, that ensures data subjects to be fully compensated for privacy violations, can be expressed by:

$$S = \tau I.$$

Substituting I with the whole indemnity function, the supply of *contractual data protection* can be written as:

$$S = \tau q L.$$

This supply of data protection can be illustrated by the market line BA in Figure *1*. Based on the assumption that our household's income can be expressed by Y_1^{NP} in case of a privacy infringement, it can be derived that for the case of intact privacy, the household's income equals Y_1^P.

The income in case of a privacy breach Y_1^{NP} is equivalent to:

$$Y_0 + qL - L - \tau qL.$$

Y_0^{NP} can be expressed by:

$$Y_0 - \tau qL.$$

The slope of line BA can be written as:

$$\frac{-(Y_1^{NP} - Y_0^{NP})}{Y_0^P - Y_1^P}.$$

The numerator is therefore equivalent to:

$$-[Y_0 + \mathrm{qL} - \mathrm{L} - \tau\mathrm{qL} - (Y_0 - \mathrm{L}) = -[\mathrm{qL}(1 - \tau)].$$

The denominator constitutes:

$$Y_0 - [Y_0 - \tau\mathrm{qL}] = \tau\mathrm{qL}.$$

The slope of the BA line thus equals:

$$\frac{-[qL(1-\tau)]}{\tau qL} = \frac{-[(1-\tau)]}{\tau}.$$

The point B in Figure *1* indicates that a household's income would not depend on the occurrence of a privacy loss and the corresponding compensation. This can be expressed by:

$$\frac{-(1-\pi)}{\pi} = \frac{-(1-\tau)}{\tau}.$$

Economically spoken, point B requires $\tau = \pi$. Data holders offering their customers *contractual data protection* would sell this level of data protection for a risk premium of $\tau\mathrm{L} = \pi\mathrm{L}$. Hence, in a competitive market, data holders would offer privacy protection schemes according to the expected losses of data breaches.

On the other side, point B would also constitute the "best option" for risk-averse data subjects in a competitive market. The highest possible indifference curve is reached at point B. Since point B is located on the 45°-line, there are no (asset) differences in case of a privacy invasion, i.e. the data subject is contractually secured that data breaches would be fully compensated. Rational and perfectly informed data subjects would demand this level of "perfect data protection" given their risk aversion. Thus, the higher data subjects estimate either the probability or the extent of a potential privacy invasion, the less they are willing to disclose their personal data as a "currency" for digital services.

Figure 3 illustrates the privacy paradox and uncertainty. By means of this figure and the two-stage-framework, the privacy paradox can be explained by three factors:

a) First, the privacy paradox can be the result of data subjects underestimating the probability of lacking data protection ($\pi^e < \pi$). The marginal rate of substitution will decrease in absolute values because of the underestimation. Graphically, the "perceived" indifference curves will be steeper (U_2' and U_3') than the "real" indifference curves (U_2 and U_3). Therefore, data subjects would choose point A without any data protection instead of the objectively better position of point B.
b) Second, the privacy paradox can be the consequence of data subjects overestimating the costs of contractual data protection. Graphically, these perceived costs can be illustrated by the line $A\mathrm{B}'$ which lies beneath the AB-line that expresses the actual costs of contractual data protection. Hence, the perceived expected utility of lacking data protection is higher than the utility of effective data protection.
c) Third, the privacy paradox can be explained by data subjects underestimating the actual extent of the privacy loss ($L^{ue} < L$). In this case, the expected utility of disclosing personal

data with an undetermined level of data protection (Point A') is higher than the actual utility with a perfect level of data protection in a competitive market (Point B).

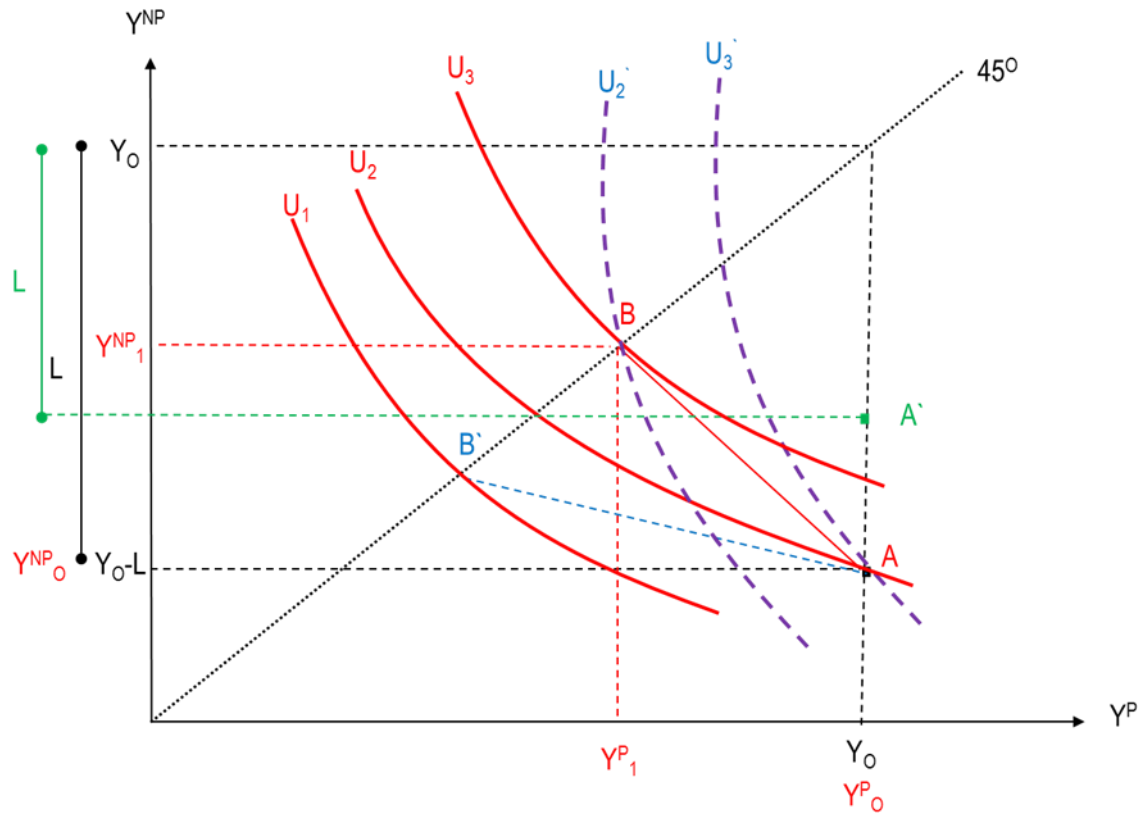

Figure 3: Privacy Paradox and Uncertainty

To summarize the preceding analysis of the two-state-of the world-model, the authors suggest that uncertainty can be a major cause for data subjects' paradoxical privacy behavior. In fact, individuals might underestimate both the scope as well as the likelihood of a data breach because of insufficient data protection. Alternatively, data subjects might overestimate the costs of contractual data protection. As a result of this three-fold uncertainty, online users might disclose their personal data for the sake of consuming allegedly "free" digital services despite

uttering privacy concerns, rather than paying a pecuniary price for online gambling or social media services.

The Privacy Paradox and the General Data Protection Regulation

Regardless, the concrete cause of the privacy paradox—bounded rationality, cognitive biases or uncertainty—it constitutes a manifestation of a "market failure" in economic terms. In the economic understanding, such a market failure justifies a regulatory intervention in the market. In light of the serious concerns about potential privacy infringements induced by ubiquitous computing,[38] policy makers have assiduously been enacting national data privacy legislations.

The current "gold standard" data privacy legislation constitutes the relatively new European General Data Protection Regulation. This regulation was finalized in 2016 in a "herculean law-making effort"[39] and became applicable law in May of 2018. The GDPR replaces the twenty-year-old and technologically outdated, or "antiquated,"[40] European Data Protection Directive[41]. The *raison d'être* of the novel regulation is the modernization and harmonization of data protection policy in the European Union.

Because of the wide territorial scope and the expanded definitions of personal data, the GDPR has a significant regulatory effect far beyond the European borders.[42] Also, the impact of the GDPR on other international privacy regulation is noteworthy. Several articles of the GDPR

[38] For a taxonomy of privacy and its infringements, see Solove.

[39] Hert and Papakonstantinou, 181.

[40] Burri and Schär, 480.

[41] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L [1995] 281/31.

[42] Goddard.

serve as blueprint for non-EU states introducing or updating their national data protection legislation.[43] Hence, some scholars term the European data privacy regulation a "historic legal milestone."[44]

The GDPR receives this recognition because it has set the bar of privacy protection to a new level. Building on the understanding that privacy constitutes a fundamental right in the EU,[45] the GDPR strengthens traditional privacy principles relating to the processing of personal data, for instance lawfulness, purpose and storage limitation, as well as data minimization.[46] Respectively, data processing is only lawful if particular prerequisites are fulfilled, inter alia data subject's consent, the existence of a contract or another legal obligation, or else greater public interests prevail.[47] The GDPR further provides data subjects with extensive and partially novel rights, such as the right to rectification, the right to erasure, the right to data portability, and the right to object.[48] The regulation also encompasses numerous obligations and new requirements for data holders, such as the designation of a data protection officer, the introduction of a voluntary code of conduct and certification scheme, the conduction of a data protection impact assessment for envisaged processing operations as well as the prerequisite of "data protection by design and by default."[49] Ultimately, rigorous liability and compensation

[43] Greenleaf.

[44] Chassang.

[45] Article 8 European Convention of Human Rights; Article 7 European Charter of Fundamental Rights.

[46] Article 5 GDPR.

[47] Article 6 GDPR.

[48] Article 16, 17, 20, 21 GDPR.

[49] Article 37 et seq, 40 et seq., 35 et seq., 25 GDPR.

payments, as well as administrative fines for unlawful conduct of data holders, reinforces the privacy rights of data subjects.[50]

Because of this new rights and remedies scheme, the GDPR constitutes a "new generation" of data protection regulation. For some scholars the regulation even poses a paradigm shift in privacy legislation, because it shifts the burden of obligation from data subjects to data holders.[51] Accordingly, individuals are no longer required to base their privacy behavior solely on their informational self-determination,[52] but can—at least in theory[53]—trust the "invisible protection" of their data on the grounds of the law.[54]

In the context of this paper, the GDPR intends to mitigate factors of uncertainty that contribute to data subjects' paradoxical privacy behavior (see "The Privacy Paradox and Uncertainty"). The primary target of the principles, rights, and remedies of the regulation is to alleviate the actual extent of a data breach that would result in an infringement of privacy. Three examples clearly demonstrate this.

[50] Article 82, 83 GDPR.

[51] Kiss and Szőke; Mayer-Schönberger.

[52] The idea of the 'right to informational self-determination' has been shaped by the German Constitutional Court in the famous 'census decision' on 15 December 1983. Based on the basic rights of human dignity and the right to free development of personality, the right to informational self-determination enables individuals to determine for themselves about the disclosure and processing of their personal data. The decision has been subjects of numerous academic commentaries that further define the right to informational self-determination, especially in the context of the digital world, see, e.g. Schwartz.

[53] Some scholars doubt the actual efficacy of the GDPR to fully protect data subjects' privacy. See, e.g. Wachter, Mittelstadt, and Floridi; Mantelero.

[54] Kiss and Szőke.

a) First, the principles of lawful, fair, and transparent data processing[55] intend to set the groundwork for effective data protection by securing contracts according the market line BA in *Figure 3*.

b) Second, the principles of purpose limitation, data minimization, data accuracy, storage limitation, integrity and confidentiality,[56] as well as the responsibility of the data holder to protect the data "by design and by default"[57] can be understood as means to avoid, or realistically, to minimize, potential losses L resulting from privacy infringements.

c) Third, the right of data portability[58] intends to encourage competition among data holders in regard to interoperable digital formats. This entrepreneurial rivalry might also foster the competitiveness for data protection, which would entail the variable τ to increase in absolute values. This, in turn, leads to a steeper market line BA in *Figure 3*. As a consequence, consuming digital services with data protection becomes cheaper for data subjects, so that remaining in point A becomes less likely.

Furthermore, consent—as grounds for lawful processing of data subjects' personal data—plays a decisive role in the GDPR,[59] especially in the context of a digital services market, and hence also for this uncertainty model. This confirmation is the manifestation of data subjects' informational self-determination reinforced by data holders accountability in the GDPR: Consent must comprise a freely given, specific, informed and unambiguous agreement of the data subject to the processing of personal data,[60] while data holders are obliged to prove the

[55] Article 5 paragraph 1 point (a) GDPR.

[56] Article 5 paragraph 1 points (b-f) GDPR.

[57] Article 25 GDPR.

[58] Article 20 GDPR.

[59] Article 6 paragraph 1 point (a) GDPR.

[60] Article 4 point (11) GDPR.

existence of this agreement at any time.[61] Thus, disclosing personal data ought to present an informed and deliberate decision of the data subject.

Figure 4 describes the role of data subjects' consent in the new uncertainty model. It illustrates two important findings:

a) The presence of statutory data protection indeed implies effective protection of a household's personal data. The loss resulting from of a privacy violation is smaller in a regulated environment than the loss sustained in an environment without data protection ($L' < L$). Although the mandatory data protection decreases the potential extent of a data breach, it does not fully eliminate it. The risk of privacy violation remains.
b) On the other hand, in a market with legally required data protection, the data subject has an economic incentive to disclose her personal data, rather than to pay a risk premium for perfect data protection while consuming digital services. Graphically, this is expressed by point A' on utility curve U_4, which is higher than point B on utility curve U_3.

Because of the remaining uncertainty in regard to the scope of a potential privacy infringement, data subjects' consent is indispensable. The process of clicking "I agree" ought to ensure that the data disclosure is a conscious choice. Data subjects are given the opportunity to personally, deliberately, and contextually assess the benefits, but also the actual risks prior to revealing their data. Based on this assessment, the data subject can decide preferences on whether to reveal data or to pay a risk premium when playing online gambling games or sending personal messages to friends on Facebook or WhatsApp.

[61] Article 7 GDPR.

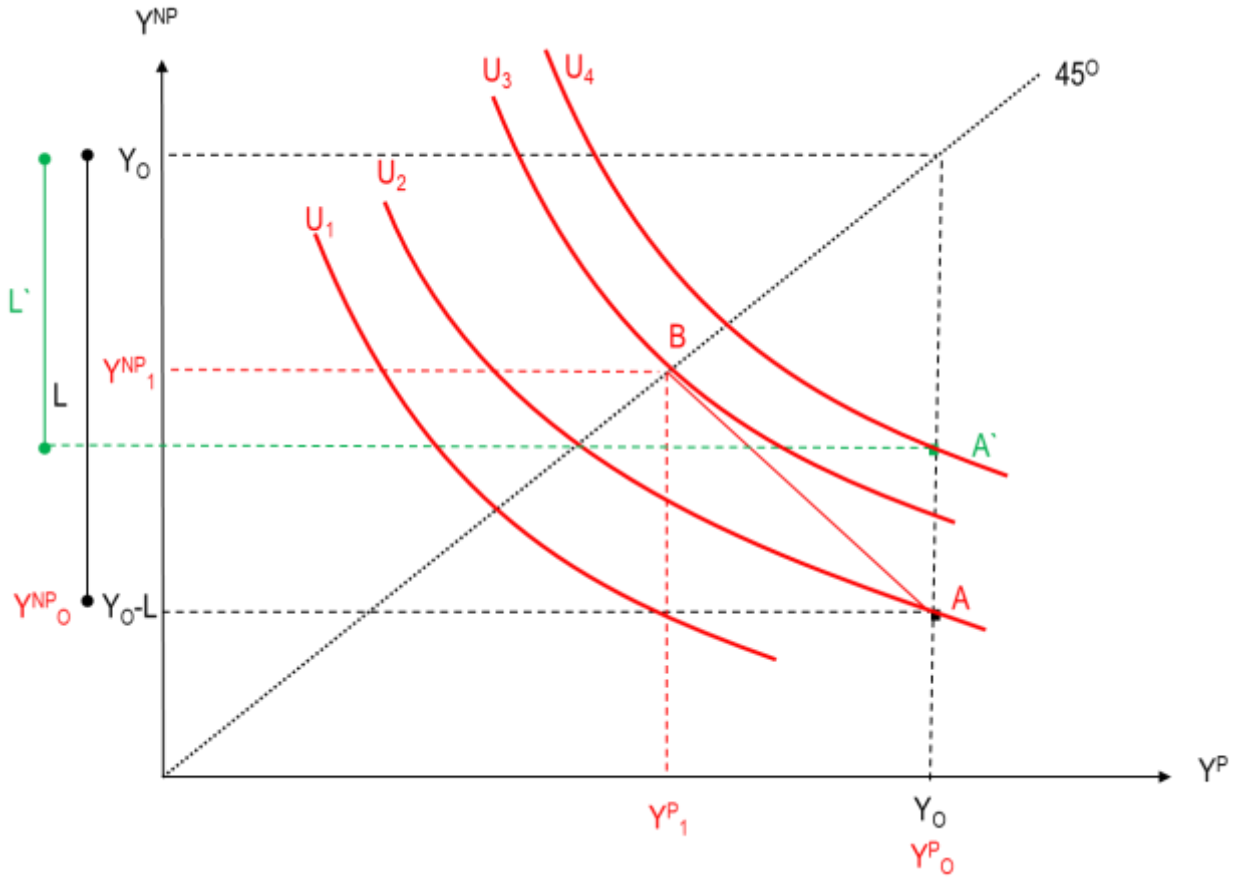

Figure 4: The role of Consent in the Uncertainty Model

In summary, privacy laws, such as the novel European General Data Protection Regulation, generally intend to strengthen the personal privacy of data subjects. In detail, this regulation aims to offset negative economic effects resulting from market failures, such as the privacy paradox. However, the regulation does not target all uncertainty factors that provoke the paradoxical privacy behavior of data subjects. The GDPR de facto primarily mitigates and compensates the extent of a data breach, yet it does not target the probability of occurrence of a privacy infringement.

If only one factor of the uncertainty product "damage * probability of damage" ($L * \pi$) is addressed, data subjects still run the risk of disclosing either too much or too little data. An underestimation of the likelihood of a data breach would entail a naïve data handling, where

data subjects disclose too much personal information. An overestimation of the probability of privacy infringement would imply an overly cautious approach of data minimization. Both approaches would be economically inefficient. The latter is, however, rather unobservable in regard to the privacy paradox. Hypothetically, if such an overestimation took place at the collective level, the political demand for data protection would induce an undifferentiated privacy law, which might wrongfully curtail the free flow of data.

Summary and Conclusions

A vast number of digital users stress that the protection of their data would be very important to them, but nevertheless disclose their data in a seemingly careless way when consuming "free" Internet services. This discrepancy in attitude and behavior has been termed privacy paradox. Numerous studies have been conducted to investigate the contradictory behavior, its occurrence, its rationale, and the potential means to conciliate it.

The privacy paradox does not only concern the academic world. It also has significant implications for modern jurisdiction and legislation. From this perspective, the question of whether online users have consciously, clearly, and unambiguously consented to barter their personal data for an online service is of utmost importance. Current examples of case law on online services, such as gambling and social media, are moving precisely in this direction. Also, contemporary data protection laws are a distinct indication of the importance of this topic. One example of such legislation is the novel European General Data Protection Regulation which strengthens the rights of data subjects and shifts the obligatory burden of privacy protection to data holders.

This article analyses the privacy paradox from an economic angle. The majority of current economic research has focused on behavioral economics to explain the discrepancy between privacy attitude and behavior. Using a two-state-of the world-model, this paper demonstrates

that the classical economic theory of uncertainty can also explain the privacy paradox. Because of diverse uncertainty factors, individuals cannot properly weigh both the expected advantages and disadvantages of either protecting or disclosing their personal data against each other. In fact, data subjects are incapable of accurately assessing the benefit of intact privacy (while paying a risk premium for digital services), against the risk of privacy infringement (with the benefit of consuming online offers for free), because they can estimate neither the extent (L) nor the probability (π) of a privacy violation.

Data privacy laws, such as the GDPR, are intended to prevent data breaches or to at least minimize harm resulting from one. Yet, in reality, this intention is only partially served. In fact, the novel European regulation is suitable to estimate both potential losses (L) and indemnity payments (I) for privacy violations and might also increase the level of competition for data protection (τ). The GDPR addresses only one crucial uncertainty factor: the extent (L) that a privacy infringement is directed. The probability (π) is not addressed. Data subjects are not able to correctly quantify the expected data protection losses (πL), and so the uncertainty that provokes the paradoxical privacy behavior remains.

Against this backdrop, the central legal role of data subjects' consent needs to be further considered. If data subjects significantly underestimate the probability of a data breach, the validity of the current form of consent is equivocal, not to say doubtful. Complex terms and conditions of interminable length followed by the "I agree" checkbox do not foster transparency, and hence do not reduce the level of data subjects' uncertainty. The conditions for consent should be construed more realistically. Instead of designing online services in such a way that would reinforce the misjudgment of data subjects' uncertainty, or to beguile them to disclose information, data holders should think of more user-friendly approaches. For example, a data holder could provide a simple, easily comprehensible, and graphically supported

explanation of why, what, how, and for how long personal data is processed and held. At that point, the declaration of consent would become economically more meaningful and legally less contestable.

Regarding the general perspective on data privacy law, it is unequivocal that we need a continuous discussion on how to make data protection more sustainable. One legal "general overhaul" every twenty years (as in the case of the GDPR) will not suffice to keep pace with the dynamic digital market. In many countries, including Germany, court rulings and subsequent reforms of general contract law have prohibited unfair terms used in standard contracts (general terms and conditions). Such clauses are generally one-sided in favor of the user of the standard contract.[62] Aren't there also rules connected with data protection? Can simply clicking on a standard declaration of consent become the basis of a contract? These simple checkboxes should be prohibited by law, as is already happening in some places in the USA.[63] Moreover, legislators should consider further means to strengthen the protection of data subjects' privacy. Besides the mere use of data protection law, privacy can be additionally enhanced by competition and consumer law, e.g. as ex ante safety regulation or as ex post liability rule.[64]

[62] Hellwege.

[63] Brown, I.

[64] Kerber; Romanosky and Acquisti.

Bibliography

Acquisti, A., and J. Grossklags. “Privacy and Rationality in Individual Decision Making.” *IEEE Security and Privacy Magazine* 3, no. 1 (2005): 26–33. doi:10.1109/MSP.2005.22.

Acquisti, Alessandro. “Privacy in Electronic Commerce and the Economics of Immediate Gratification.” In *Proceedings of the 5th ACM Conference on Electronic Commerce (EC '04)*. Edited by Jack Breese, Joan Feigenbaum and Margo Seltzer, 21. New York, New York, USA: ACM Press, 2004.

Acquisti, Alessandro, and Ralph Gross. “Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook.” In *Privacy Enhancing Technologies.* Vol. 4258. Edited by David Hutchison et al., 36–58. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006.

Acquisti, Alessandro, and Jens Grossklags. “Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting.” In *Economics of Information Security.* Vol. 12. Edited by L. J. Camp and Stephen Lewis, 165–78. Advances in Information Security. Boston: Kluwer Academic Publishers, 2004.

Acquisti, Alessandro, Leslie K. John, and George Loewenstein. “The Impact of Relative Standards on the Propensity to Disclose.” *Journal of Marketing Research* 49, no. 2 (2012): 160–74. doi:10.1509/jmr.09.0215.

Anderson, Catherine L., and Ritu Agarwal. “The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information.” *Information Systems Research* 22, no. 3 (2011): 469–90. doi:10.1287/isre.1100.0335.

Baek, Young Min. “Solving the Privacy Paradox: A Counter-Argument Experimental Approach.” *Computers in Human Behavior* 38 (2014): 33–42. doi:10.1016/j.chb.2014.05.006.

Baek, Young Min, Eun-mee Kim, and Young Bae. “My Privacy Is Okay, but Theirs Is Endangered: Why Comparative Optimism Matters in Online Privacy Concerns.” *Computers in Human Behavior* 31 (2014): 48–56. doi:10.1016/j.chb.2013.10.010.

Barnes, Susan B. “A Privacy Paradox: Social Networking in the United States.” *First Monday* 11, no. 9 (2006). doi:10.5210/fm.v11i9.1394.

Barth, Susanne, and Menno D.T. de Jong. “The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – a Systematic Literature Review.” *Telematics and Informatics* 34, no. 7 (2017): 1038–58. doi:10.1016/j.tele.2017.04.013.

Bashir, Masooda, Carol Hayes, April D. Lambert, and Jay P. Kesan. “Online Privacy and Informed Consent: The Dilemma of Information Asymmetry.” *Proceedings of the Association for Information Science and Technology* 52, no. 1 (2015): 1–10. doi:10.1002/pra2.2015.145052010043.

Berendt, Bettina, Oliver Günther, and Sarah Spiekermann. “Privacy in E-Commerce: Stated Preferences Vs. Actual Behavior.” *Communications of the ACM* 48, no. 4 (2005): 101–6. doi:10.1145/1053291.1053295.

Beresford, Alastair R., Dorothea Kübler, and Sören Preibusch. “Unwillingness to Pay for Privacy: A Field Experiment.” *Economics Letters* 117, no. 1 (2012): 25–27. doi:10.1016/j.econlet.2012.04.077. http://www.sciencedirect.com/science/article/pii/S0165176512002182.

Boyles, Jan Lauren, Aaron Smith, and Mary Madden. “Privacy and Data Management on Mobile Devices.” Accessed March 3, 2019. http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx.

Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. “Misplaced Confidences.” *Social Psychological and Personality Science* 4, no. 3 (2013): 340–47. doi:10.1177/1948550612455931.

Brown, Barry. “Studying the Internet Experience.” Accessed March 3, 2019. http://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf.

Brown, Ian. “The Economics of Privacy, Data Protection and Surveillance.” In *Handbook on the Economics of the Internet*. Edited by Johannes M. Bauer and Michael Latzer, 247–61. Cheltenham, UK, Northampton, MA: Edward Elgar Publishing, 2016.

Buck, Christoph, Chris Horbel, Claas Christian Germelmann, and Torsten Eymann. “The Unconscious App Consumer: Discovering and Comparing the Information-Seeking Patterns Among Mobile Application Consumers.” In *Proceedings of the 22nd European Conference on Information Systems (ECIS '14).*, 2014.

Burri, and Schär. “The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy.” *Journal of Information Policy* 6 (2016): 479. doi:10.5325/jinfopoli.6.2016.0479.

Carrascal, Juan Pablo, Christopher Riederer, Vijay Erramilli, Mauro Cherubini, and Rodrigo de Oliveira. “Your Browsing Behavior for a Big Mac.” In *Proceedings of the 22nd International Conference on World Wide Web (WWW '13)*. Edited by Daniel Schwabe et al., 189–200. New York, New York, USA: ACM Press, 2013.

Chassang, Gauthier. “The Impact of the EU General Data Protection Regulation on Scientific Research.” *Ecancermedicalscience* 11 (2017): 709. doi:10.3332/ecancer.2017.709.

Chellappa, Ramnath K., and Raymond G. Sin. “Personalization Versus Privacy: An Empirical Examination of the Online Consumer’s Dilemma.” *Information Technology and Management* 6, 2-3 (2005): 181–202. doi:10.1007/s10799-005-5879-y.

Chen, Hsuan-Ting. “Revisiting the Privacy Paradox on Social Media with an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management.” *American Behavioral Scientist* 62, no. 10 (2018): 1392–1412. doi:10.1177/0002764218792691.

Chen, Zhen Troy, and Ming Cheung. “Privacy Perception and Protection on Chinese Social Media: A Case Study of WeChat.” *Ethics and Information Technology* 20, no. 4 (2018): 279–89. doi:10.1007/s10676-018-9480-6.

Cho, Hichang, Jae-Shin Lee, and Siyoung Chung. “Optimistic Bias About Online Privacy Risks: Testing the Moderating Effects of Perceived Controllability and Prior Experience.” *Computers in Human Behavior* 26, no. 5 (2010): 987–95. doi:10.1016/j.chb.2010.02.012.

Cullis, John G., and Philip R. Jones. *Microeconomics Through Life's Decisions*. Harlow: Financial Times/Prentice Hall, 2009.

Culnan, Mary J., and Pamela K. Armstrong. “Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation.” *Organization Science* 10, no. 1 (1999): 104–15. doi:10.1287/orsc.10.1.104.

Debatin, Bernhard, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. “Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences.” *Journal of Computer-Mediated Communication* 15, no. 1 (2009): 83–108. doi:10.1111/j.1083-6101.2009.01494.x.

Dienlin, Tobias, and Miriam J. Metzger. “An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample.” *Journal of Computer-Mediated Communication* 21, no. 5 (2016): 368–83. doi:10.1111/jcc4.12163.

Dienlin, Tobias, and Sabine Trepte. “Is the Privacy Paradox a Relic of the Past? An in-Depth Analysis of Privacy Attitudes and Privacy Behaviors.” *European Journal of Social Psychology* 45, no. 3 (2015): 285–97. doi:10.1002/ejsp.2049.

Dinev, Tamara, Massimo Bellotto, Paul Hart, Vincenzo Russo, Ilaria Serra, and Christian Colautti. “Privacy Calculus Model in E-Commerce – a Study of Italy and the United States.” *European Journal of Information Systems* 15, no. 4 (2006): 389–402. doi:10.1057/palgrave.ejis.3000590.

Dinev, Tamara, and Paul Hart. “An Extended Privacy Calculus Model for E-Commerce Transactions.” *Information Systems Research* 17, no. 1 (2006): 61–80. doi:10.1287/isre.1060.0080.

Domo. “Data Never Sleeps 7.0.” Accessed May 10, 2020. https://www.domo.com/learn/data-never-sleeps-7.

D'Souza, Giles, and Joseph E. Phelps. “The Privacy Paradox: The Case of Secondary Disclosure.” *Review of Marketing Science* 7, no. 1 (2009). doi:10.2202/1546-5616.1072.

Ellison, Nicole B., Jessica Vitak, Charles Steinfield, Rebecca Gray, and Cliff Lampe. “Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment.” In *Privacy Online*. Edited by Sabine Trepte and Leonard Reinecke, 19–32. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

Facebook. Bundeskartellamt, February 15, 2019. Accessed April 15, 2020. https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3591568.

Facebook. Oberlandesgericht Düsseldorf, August 26, 2019.

Fashion ID. European Court of Justice, July 29, 2019. Accessed April 15, 2020. http://curia.europa.eu/juris/liste.jsf?language=de&num=C-40/17.

Gambino, Andrew, Jinyoung Kim, S. Shyam Sundar, Jun Ge, and Mary Beth Rosson. “User Disbelief in Privacy Paradox.” In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. Edited by Jofish Kaye et al., 2837–43. New York, New York, USA: ACM Press, 2016.

Gerber, Nina, Paul Gerber, and Melanie Volkamer. “Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior.” *Computers & Security* 77 (2018): 226–61. doi:10.1016/j.cose.2018.04.002.

Gewinnspiel. Oberlandesgericht Frankfurt am Main, June 27, 2019.

Gimpel, Henner, Dominikus Kleindienst, and Daniela Waldmann. “The Disclosure of Private Data: Measuring the Privacy Paradox in Digital Services.” *Electronic Markets* 28, no. 4 (2018): 475–90. doi:10.1007/s12525-018-0303-8.

Goddard, Michelle. “The EU General Data Protection Regulation (GDPR): European Regulation That Has a Global Impact.” *International Journal of Market Research* 59, no. 6 (2017): 703–5. doi:10.2501/IJMR-2017-050.

Greenleaf, Graham. “Global Data Privacy Laws 2019: 132 National Laws & Many Bills (6th Ed January 2019): Supplement to 157 Privacy Laws & Business International Report.” *SSRN Journal*, 9 February 2019.

Gruzd, Anatoliy, and Ángel Hernández-García. “Privacy Concerns and Self-Disclosure in Private and Public Uses of Social Media.” *Cyberpsychology, behavior and social networking* 21, no. 7 (2018): 418–28. doi:10.1089/cyber.2017.0709.

Hann, Il-Horn, Kai-Lung Hui, Tom Lee, and Ivan Png. “Online Information Privacy: Measuring the Cost-Benefit Trade-Off.” In *Proceedings of the 23rd International Conference on Information Systems (ICIS '02)*., 2002.

Hargittai, Eszter, and Alice Marwick. “"What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy.” *International Journal of Communication* 10 (2016): 3737–57. Accessed March 3, 2019. https://ijoc.org/index.php/ijoc/article/view/4655/1738.

Hellwege, Phillip. *Allgemeine Geschäftsbedingungen, Einseitig Gestellte Vertragsbedingungen Und Die Allgemeine Rechtsgeschäftslehre*. Mohr Siebeck, 2010. doi:10.1628/978-3-16-151225-4.

Heravi, Alireza, Sameera Mubarak, and Kim-Kwang Raymond Choo. “Information Privacy in Online Social Networks: Uses and Gratification Perspective.” *Computers in Human Behavior* 84 (2018): 441–59. doi:10.1016/j.chb.2018.03.016.

Hert, Paul de, and Vagelis Papakonstantinou. “The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?” *Computer Law & Security Review* 32, no. 2 (2016): 179–94. doi:10.1016/j.clsr.2016.02.006.

Hew, Jun-Jie, Garry Wei-Han Tan, Binshan Lin, and Keng-Boon Ooi. “Generating Travel-Related Contents Through Mobile Social Tourism: Does Privacy Paradox Persist?” *Telematics and Informatics* 34, no. 7 (2017): 914–35. doi:10.1016/j.tele.2017.04.001.

Hoffmann, Christian Pieter, Christoph Lutz, and Giulia Ranzini. “Privacy Cynicism: A New Approach to the Privacy Paradox.” *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10, no. 4 (2016). doi:10.5817/CP2016-4-7.

Hoofnagle, Chris, Ashkan Soltani, Nathaniel Good, and Dietrich Wambach. “Behavioral Advertising: The Offer You Cannot Refuse.” *Harvard Law & Policy Review* 6 (2012): 273–96. https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3086&context=facpubs.

Hoofnagle, Chris Jay, and Jennifer M. Urban. “Alan Westin's Privacy Homo Economicus.” *Wake Forest Law Review* 40 (2014): 261–317. Accessed March 3, 2019. https://www.ftc.gov/system/files/documents/public_comments/2015/09/00003-97143.pdf.

Huberman, B. A., E. Adar, and L. R. Fine. “Valuating Privacy.” *IEEE Security and Privacy Magazine* 3, no. 5 (2005): 22–25. doi:10.1109/MSP.2005.137.

Ipsos. “CIGI-Ipsos Global Survey on Internet Security and Trust: Part I & II: Internet Security, Online Privacy & Trust.” Accessed May 10, 2020. https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-%20Part%201%20%26%202%20Internet%20Security%2C%20Online%20Privacy%20%26%20Trust.pdf.

Jehovan Todistajat. European Court of Justice, July 10, 2018. Accessed June 1, 2020. http://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1.

Jensen, Carlos, Colin Potts, and Christian Jensen. “Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior.” *International Journal of Human-Computer Studies* 63, 1-2 (2005): 203–27. doi:10.1016/j.ijhcs.2005.04.019.

Jentzsch, Nicola. “State-of-the-Art of the Economics of Cyber-Security and Privacy.” Accessed February 9, 2018. https://www.econstor.eu/bitstream/10419/126223/1/Jentzsch_2016_State-Art-Economics.pdf.

Jiang, Zhenhui, Cheng Suang Heng, and Ben C. F. Choi. “Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions.” *Information Systems Research* 24, no. 3 (2013): 579–95. doi:10.1287/isre.1120.0441.

John, Leslie K., Alessandro Acquisti, and George Loewenstein. “Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information.” *Journal of Consumer Research* 37, no. 5 (2011): 858–73. doi:10.1086/656423.

Kehr, Flavius, Tobias Kowatsch, Daniel Wentzel, and Elgar Fleisch. “Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus.” *Information Systems Journal* 25, no. 6 (2015): 607–35. doi:10.1111/isj.12062.

Kehr, Flavius, Daniel Wentzel, and Tobias Kowatsch. “Privacy Paradox Revised: Pre-Existing Attitudes, Psychological Ownership, and Actual Disclosure.” *Thirty Fifth International Conference on Information Systems, Auckland, New Zealand*, 2014, 1–12. Accessed March 3, 2018. https://www.alexandria.unisg.ch/242216/.

Kehr, Flavius, Daniel Wentzel, and Peter Mayer. “Rethinking the Privacy Calculus: On the Role of Dispositional Factors and Affect.” *Reshaping society through information systems design International Conference on Information Systems (ICIS 2013); Milan, Italy, 15 - 18 December 2013* 4 (2013): 3355–64.

Keith, Mark J., Samuel C. Thompson, Joanne Hale, Paul Benjamin Lowry, and Chapman Greer. “Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior.” *International Journal of Human-Computer Studies* 71, no. 12 (2013): 1163–73. doi:10.1016/j.ijhcs.2013.08.016.

Kerber, Wolfgang. “Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection.” *Journal of Intellectual Property Law & Practice*, 2016, jpw150. doi:10.1093/jiplp/jpw150.

Kiss, Attila, and Gergely László Szőke. “Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation.” In *Reforming European Data Protection Law.* Vol. 20. Edited by Serge Gutwirth, Ronald Leenes and Paul de Hert, 311–31. Law, Governance and Technology Series. Dordrecht: Springer Netherlands, 2015.

Knijnenburg, Bart P., Alfred Kobsa, and Hongxia Jin. “Counteracting the Negative Effect of Form Auto-Completion on the Privacy Calculus.” In *Proceedings of the 34th International Conference on Information Systems (ICIS '13).*, 2013.

Kokolakis, Spyros. “Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon.” *Computers & Security* 64 (2017): 122–34. doi:10.1016/j.cose.2015.07.002.

Lee, Haein, Hyejin Park, and Jinwoo Kim. “Why Do People Share Their Context Information on Social Network Services? A Qualitative Study and an Experimental Study on Users' Behavior of Balancing Perceived Benefit and Risk.” *International Journal of Human-Computer Studies* 71, no. 9 (2013): 862–77. doi:10.1016/j.ijhcs.2013.01.005.

Li, Han, Rathindra Sarathy, and Heng Xu. “Understanding Situational Online Information Disclosure as a Privacy Calculus.” *Journal of Computer Information Systems* 51, no. 1 (2010): 62–71.

Mantelero, Alessandro. “The Future of Consumer Data Protection in the E.U. Re-Thinking the “Notice and Consent” Paradigm in the New Era of Predictive Analytics.” *Computer Law & Security Review* 30, no. 6 (2014): 643–60. doi:10.1016/j.clsr.2014.09.004.

Mayer-Schönberger, Viktor. “Generational Development of Data Protection in Europe.” In *Technology and Privacy: The New Landscape*. Edited by Marc Rotenberg and Philip E. Agre, 219–41. Cambridge: MIT Press, 2015.

McDonald, Aleecia, and Lorrie Cranor. “Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising.” Accessed March 3, 2019. http://ssrn.com/abstract=1989092.

McDonald, Aleecia M., and Lorrie Faith Cranor. “The Cost of Reading Privacy Policies.” *I/S: A Journal of Law and Policy for the Information*, 4, no. 3 (2008): 540–65.

Miltgen, Caroline Lancelot, and Dominique Peyrat-Guillard. “Cultural and Generational Influences on Privacy Concerns: A Qualitative Study in Seven European Countries.” *European Journal of Information Systems* 23, no. 2 (2014): 103–25. doi:10.1057/ejis.2013.17.

Mothersbaugh, David L., William K. Foxx, Sharon E. Beatty, and Sijun Wang. “Disclosure Antecedents in an Online Service Context.” *Journal of Service Research* 15, no. 1 (2012): 76–98. doi:10.1177/1094670511424924.

Nofer, Michael, Oliver Hinz, Jan Muntermann, and Heiko Roßnagel. “The Economic Impact of Privacy Violations and Security Breaches.” *Business & Information Systems Engineering* 6, no. 6 (2014): 339–48. doi:10.1007/s12599-014-0351-3.

Norberg, Patricia A., Daniel R. Horne, and David A. Horne. “The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors.” *The Journal of Consumer Affairs* 41, no. 1 (2007): 100–126.

OECD. “Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value.” *OECD Digital Economy Papers* 2013, no. 220. https://doi.org/10.1787/5k486qtxldmq-en.

Pentina, Iryna, Lixuan Zhang, Hatem Bata, and Ying Chen. “Exploring Privacy Paradox in Information-Sensitive Mobile App Adoption: A Cross-Cultural Comparison.” *Computers in Human Behavior* 65 (2016): 409–19. doi:10.1016/j.chb.2016.09.005.

Planet49. European Court of Justice, October 1, 2020. Accessed April 15, 2020. http://curia.europa.eu/juris/liste.jsf?language=de&num=C-673/17.

Reynolds, Bernardo, Jayant Venkatanathan, Jorge Gonçalves, and Vassilis Kostakos. “Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours.” In *Human-Computer Interaction – INTERACT 2011*. Vol. 6948. Edited by David Hutchison et al., 204–15. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

Romanosky, Sasha, and Allessandro Acquisti. “Privacy Costs and Personal Data Protection: Economic and Legal Perspectives.” *Berkeley Tech*, no. 24 (2009): 1062–91. Accessed May 10, 2020. https://www.heinz.cmu.edu/~acquisti/papers/RomanoskyAcquisti-INFORMS-2009.pdf.

Schwartz, Paul M. “Property, Privacy, and Personal Data.” *Harvard Law Review* 117 (2004): 2055–2128.

Shklovski, Irina, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. “Leakiness and Creepiness in App Space.” In *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems (CHI '14)*. Edited by Matt Jones et al., 2347–56. New York, New York, USA: ACM Press, 2014.

Solove, Daniel J. “A Taxonomy of Privacy.” *University of Pennsylvania Law Review* 154, no. 3 (January 2006): 477–560.

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. “E-Privacy in 2nd Generation E-Commerce.” In *Proceedings of the 3rd ACM Conference on Electronic Commerce (EC '01)*. Edited by Michael P. Wellman and Yoav Shoham, 38–47. New York, New York, USA: ACM Press, 2001.

Sundar, S. Shyam, Hyunjin Kang, Mu Wu, Eun Go, and Bo Zhang. “Unlocking the Privacy Paradox.” In *CHI '13 Extended Abstracts on Human Factors in Computing Systems on - CHI EA '13*. Edited by Wendy E. Mackay, Stephen Brewster and Susanne Bødker, 811. New York, New York, USA: ACM Press, 2013.

Taddicken, Monika. “The ‘Privacy Paradox’ in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure.” *Journal of Computer-Mediated Communication* 19, no. 2 (2014): 248–73. doi:10.1111/jcc4.12052.

Tufekci, Zeynep. “Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites.” *Bulletin of Science, Technology & Society* 28, no. 1 (2008): 20–36. doi:10.1177/0270467607311484.

Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation.” *International Data Privacy Law* 7, no. 2 (2017): 76–99. doi:10.1093/idpl/ipx005.

Wakefield, Robin. “The Influence of User Affect in Online Information Disclosure.” *The Journal of Strategic Information Systems* 22, no. 2 (2013): 157–74. doi:10.1016/j.jsis.2013.01.003.

Williams, Meredydd, Jason R. C. Nurse, and Sadie Creese. “Privacy Is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things.” In *Proceedings of the 15th Annual Conference on Privacy, Security and Trust (PST '17)*, 181–18109. IEEE, 2017.

Wilson, David W., and Joseph S. Valacich. “Unpacking the Privacy Paradox: Irrational Decision-Making Within the Privacy Calculus.” In *Proceedings of the 33rd International Conference on Information Systems (ICIS '12)*. Vol. 5, 4152–62., 2012.

Wirtschaftsakademie Schleswig-Holstein. European Court of Justice, June 5, 2018. Accessed June 1, 2020. http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2297912.

Xu, Heng, Hock-Hai Teo, Bernard C. Y. Tan, and Ritu Agarwal. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services." *Journal of Management Information Systems* 26, no. 3 (2009): 135–74. doi:10.2753/MIS0742-1222260305.

Young, Alyson Leigh, and Anabel Quan-Haase. "PRIVACY PROTECTION STRATEGIES on FACEBOOK." *Information, Communication & Society* 16, no. 4 (2013): 479–500. doi:10.1080/1369118X.2013.777757.

Working Paper Series in Economics

(recent issues)

No. 392 *Mats P. Kahl:* Impact of Cross-Border Competition on the German Retail Gasoline Market – German-Polish Border, July 2020

No. 391 *John P. Weche and Joachim Wagner:* Markups and Concentration in the Context of Digitization: Evidence from German Manufacturing Industries, July 2020

No. 390 *Thomas Wein:* Cartel behavior and efficient sanctioning by criminal sentences, July 2020

No. 389 *Christoph Kleineberg.* Market definition of the German retail gasoline industry on highways and those in the immediate vicinity, July 2020

No. 388 *Institut für Volkswirtschaftslehre:* Forschungsbericht 2019, Januar 2020

No. 387 *Boris Hirsch, Elke J. Jahn, and Thomas Zwick.* Birds, Birds, Birds: Co-worker Similarity, Workplace Diversity, and Voluntary Turnover, May 2019

No. 386 *Joachim Wagner:* Transaction data for Germany's exports and imports of goods, May 2019

No. 385 *Joachim Wagner:* Export Scope and Characteristics of Destination Countries: Evidence from German Transaction Data, May 2019

No. 384 *Antonia Arsova:* Exchange rate pass-through to import prices in Europe: A panel cointegration approach, February 2019

No. 383 *Institut für Volkswirtschaftslehre:* Forschungsbericht 2018, Januar 2019

No. 382 *Jörg Schwiebert*: A Sample Selection Model for Fractional Response Variables, April 2018

No. 381 *Jörg Schwiebert*: A Bivarate Fractional Probit Model, April 2018

No. 380 *Boris Hirsch and Steffen Mueller:* Firm wage premia, industrial relations, and rent sharing in Germany, February 2018

No. 379 *John P. Weche and Achim Wambach:* The fall and rise of market power in Europe, January 2018

No.378: *Institut für Volkswirtschaftslehre:* Forschungsbericht 2017, Januar 2018

No.377: *Inna Petrunyk and Christian Pfeifer:* Shortening the potential duration of unemployment benefits and labor market outcomes: Evidence from a natural experiment in Germany, January 2018

No.376: *Katharina Rogge, Markus Groth und Roland Schuhr:* Offenlegung von CO2-Emissionen und Klimastrategien der CDAX-Unternehmen – eine statistische Analyse erklärender Faktoren am Beispiel der CDP-Klimaberichterstattung, Oktober 2017

No.375: *Christoph Kleineberg und Thomas Wein:* Verdrängungspreise an Tankstellen?, September 2017

No.374: *Markus Groth, Laura Schäfer und Pia Scholz*: 200 Jahre „On the Principles of Political Economy and Taxation" – Eine historische Einordnung und Würdigung, März 2017

No.373: *Joachim Wagner:* It pays to be active on many foreign markets - Profitability in German multi-market exporters and importers from manufacturing industries, March 2017

No.372: *Joachim Wagner:* Productivity premia for many modes of internationalization - A replication study of Békes / Muraközy, Economics Letters (2016), March 2017 [published in: International Journal for Re-Views in Empirical Economics - IREE, Vol. 1 (2017-4)]

No.371: *Marius Stankoweit, Markus Groth and Daniela Jacob:* On the Heterogeneity of the Economic Value of Electricity Distribution Networks: an Application to Germany, March 2017

No.370: *Joachim Wagner:* Firm size and the use of export intermediaries. A replication study of Abel-Koch, The World Economy (2013), January 2017 [published in: International Journal for Re-Views in Empirical Economics - IREE, Vol. 1 (2017-1)]

No.369: *Joachim Wagner:* Multiple import sourcing First evidence for German enterprises from manufacturing industries, January 2017 [published in : Open Economies Review 29 (2018), 1, 165-175]

No.368: *Joachim Wagner:* Active on many foreign markets A portrait of German multi-market exporters and importers from manufacturing industries, January 2017 [published in: Jahrbücher für Nationalökonomie und Statistik 238 (2018), 2, 157-182]

No.367: *Institut für Volkswirtschaftslehre:* Forschungsbericht 2016, Januar 2017

No.366: *Tim W. Dornis and Thomas Wein:* Trademarks, Comparative Advertising, and Product Imitations: An Untold Story of Law and Economics, September 2016

No.365: *Joachim Wagner:* Intra-good trade in Germany: A first look at the evidence, August 2016 [published in: Applied Economics 49 (2017), 57, 5753-5761]

No.364: *Markus Groth and Annette Brunsmeier:* A cross-sectoral analysis of climate change risk drivers based on companies' responses to the CDP's climate change information request, June 2016

No.363: *Arne Neukirch and Thomas Wein:* Collusive Upward Gasoline Price Movements in Medium-Sized German Cities, June 2016

No.362: *Katja Seidel:* Job Characteristics and their Effect on the Intention to Quit Apprenticeship., May 2016

No.361: *Katja Seidel:* Apprenticeship: The Intention to Quit and the Role of Secondary Jobs in It., May 2016

No.360: *Joachim Wagner:* Trade costs shocks and lumpiness of imports: Evidence from the Fukushima disaster, May 2016 [published in: Economics Bulletin 37 (2017), 1, 149-155]

No.359: *Joachim Wagner:* The Lumpiness of German Exports and Imports of Goods, April 2016 [published in: Economics - The Open-Access, Open-Assessment E-Journal 10, 2016-21]

No.358: *Ahmed Fayez Abdelgouad:* Exporting and Workforce Skills-Intensity in the Egyptian Manufacturing Firms: Empirical Evidence Using World Bank Firm-Level Data for Egypt, April 2016

No.357: *Antonia Arsova and Deniz Dilan Karaman Örsal:* An intersection test for the cointegrating rank in dependent panel data, March 2016

No.356: *Institut für Volkswirtschaftslehre:* Forschungsbericht 2015, Januar 2016

No.355: *Christoph Kleineberg and Thomas Wein:* Relevance and Detection Problems of Margin Squeeze – The Case of German Gasoline Prices, December 2015

No.354: *Karsten Mau:* US Policy Spillover(?) - China's Accession to the WTO and Rising Exports to the EU, December 2015

No.353: *Andree Ehlert, Thomas Wein and Peter Zweifel:* Overcoming Resistance Against Managed Care – Insights from a Bargaining Model, December 2015

No.352: *Arne Neukirch und Thomas Wein:* Marktbeherrschung im Tankstellenmarkt - Fehlender Binnen- und Außenwettbewerb an der Tankstelle? Deskriptive Evidenz für Marktbeherrschung, Dezember 2015

No.351: *Jana Stoever and John P. Weche:* Environmental regulation and sustainable competitiveness: Evaluating the role of firm-level green investments in the context of the Porter hypothesis, November 2015

No.350: *John P. Weche:* Does green corporate investment really crowd out other business investment?, November 2015

No.349: *Deniz Dilan Karaman Örsal and Antonia Arsova:* Meta-analytic cointegrating rank tests for dependent panels, November 2015

No.348: *Joachim Wagner:* Trade Dynamics and Trade Costs: First Evidence from the Exporter and Importer Dynamics Database for Germany, October 2015 [published in: Applied Economics Quarterly 63 (2017), 2, 137-159]

No.347: *Markus Groth, Maria Brück and Teresa Oberascher:* Climate change related risks, opportunities and adaptation actions in European cities – Insights from responses to the CDP cities program, October 2015

No.346: *Joachim Wagner:* 25 Jahre Nutzung vertraulicher Firmenpaneldaten der amtlichen Statistik für wirtschaftswissenschaftliche Forschung: Produkte, Projekte, Probleme, Perspektiven, September 2015 [publiziert in: AStA Wirtschafts- und Sozialstatistisches Archiv 9 (2015), 2, 83-106]

No.345: *Christian Pfeifer:* Unfair Wage Perceptions and Sleep: Evidence from German Survey Data, August 2015

No.344: *Joachim Wagner:* Share of exports to low-income countries, productivity, and innovation: A replication study with firm-level data from six European countries, July 2015 [published in: Economics Bulletin 35 (2015), 4, 2409-2417]

No.343: *Joachim Wagner:* R&D activities and extensive margins of exports in manufacturing enterprises: First evidence for Germany, July 2015 [published in: The International Trade Journal 31 (2017), 3, 232-244]

No.342: *Joachim Wagner:* A survey of empirical studies using transaction level data on exports and imports, June 2015 [published in: Review of World Economics 152 (2016), 1, 215-225]

No.341: *Joachim Wagner:* All Along the Data Watch Tower - 15 Years of European Data Watch in Schmollers Jahrbuch, June 2015 [published in: Schmollers Jahrbuch / Journal of Applied Social Science Studies 135 (2015), 3, 401-410]

No.340: *Joachim Wagner:* Kombinierte Firmenpaneldaten – Datenangebot und Analyse-potenziale, Mai 2015 [publiziert in: S. Liebig et al. (Hrsg.), Handbuch Empirische Organisationsforschung, Wiesbaden: Springer Fachmedien 2017, S. 63-74]

(see www.leuphana.de/institute/ivwl/publikationen/working-papers.html for a complete list)

Leuphana Universität Lüneburg
Institut für Volkswirtschaftslehre
Postfach 2440
D-21314 Lüneburg
Tel.: ++49 4131 677 2321
email: maike.mente@leuphana.de

www.leuphana.de/institute/ivwl/forschung/working-papers.html