I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Coercing Online Privacy[2]

DR. BARBARA SANDFUCHS, UNIVERSITY OF PASSAU

DR. ANDREAS KAPSNER, LUDWIG-MAXIMILIANS-UNIVERSITÄT MUNICH

Abstract: Despite all advantages, online self-disclosure can cause harms to the development of the users' personality. Hence, governments around the world, including the German and the U.S. governments, may feel a need to compel or nudge users into revealing less and thereby protect users from their own mistakes. However, the paper will argue both that governments are neither obliged nor allowed to prevent competent adult users from voluntary online self-disclosure by paternalistic interventions that only aim to protect the users. These findings extend to the approach of using nudges to correct irrational behavior, discussed with particular intensity in current U.S. scholarship. Instead, the paper suggests alternative paths to protect users from disadvantageous, but voluntary self-disclosure while respecting the users' autonomy and constitutional rights.

A. INTRODUCTION

"Privacy is not an optional good, like a second home or an investment account" (Anita L. Allen)[2]

---

[1] The title pays tribute to Anita L. Allen, *Coercing Privacy,* 40 WM. & MARY L. REV. 723 (1999). For a broader discussion of the legal requirements to coerce online privacy, see BARBARA SANDFUCHS, PRIVATHEIT WIDER WILLEN? (2015).

[2] *See* Anita L. Allen, *Coercing Privacy,* 40 WM. & MARY L. REV. 723, 740 (1999).

In today's society, competent adult internet users voluntarily disclose vast amounts of data about themselves. This may lead to numerous advantages, such as economic benefits or increased convenience. Nevertheless such voluntary behavior can cause great harm to the users (see B).

Governments[3] may feel that by relatively small interventions they could protect their citizens from acts of self-disclosure which are not in the users' best interest. They could take the role of a nanny, balance the pros and cons of certain forms of self-disclosure, and prevent self-disclosures that result in more disadvantages than advantages for the users. But, must they do so? May they do so? And if not, are they left with tied hands?

Courts both in Germany and in the United States regularly reject limitations on the freedoms of competent adult individuals, unless their behavior causes harms to others or the society. The question will thus be: are the harms inflicted by careless self-disclosure great enough to warrant government intervention?

When investigating these questions, it seems promising to follow a comparative approach by examining Germany as one of the most influential and traditionally privacy-friendly jurisdictions within the European Union, and at the United States as the base of the leading online businesses, such as Google, Facebook, Apple, and Microsoft.

This paper focuses on online privacy, understood as informational privacy in the online environment.[4] For the purpose of the following research, informational privacy shall mean the individual's right to informational self-determination, that is, the right to decide personally about the disclosure and application of their personal data.

Online privacy can be compromised by two kinds of voluntary online self-disclosure. One way is by means of explicit disclosure, such

---

[3] For the purpose of this paper, the term "government" is meant not to be limited to the executive branch, but to include all public actors both on the federal and (with exceptions) on the state level.

[4] Disclaimer: This paper does not attempt to present a universal definition of privacy, but only aims at determining a workable approach. *See* Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 393 (1978) ("The concept of 'privacy' is elusive and ill defined. Much ink has been spilled in trying to clarify its meaning." Though countless scholars have contributed to the debate about privacy, this statement from 1978 is still valid today. The various characterizations that have been suggested, such as privacy as secrecy, as control over personal data, as limited access to persons or simply as intimacy all leave out important aspects or are too broad, in most cases both); *see also* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2009) (gives an extensive critique of these conceptions and an account of privacy as a nexus of many concepts that share a Wittgensteinian family resemblance).

as adding personal information to profiles in social networks, to blogs, or to personal websites. Explicit disclosure occurs intentionally and purposefully. The other way, which is of greater impact, is through implicit disclosure. The use of almost any kind of online service is accompanied by the collection, storage and aggregation of vast amounts of data, for example about the users' browsing and online shopping activities. Among other things, these data are used to provide users with future online experiences according to their preferences. Storing IP-addresses, placing cookies, using web-bugs, java script tags, as well as browser and OS fingerprints allows the website operators and third parties to track the users' online behavior. These data can then be used to generate information about the users.[5]

Comparing their data with existing databases allows the discovery of correlations and behavior patterns that the users themselves are often unaware of. These can be used to predict future activities and preferences.[6] Even though implicit self-disclosure is not usually intended by users, it is based on their active use of a website or service which processes data or allows third parties to do so.

When disclosing data both in explicit and implicit ways, users are often not aware of all relevant information regarding the consequences of the self-disclosure. For example, users regularly do not read all relevant privacy policies as well as other types of standard terms of contract.[7] However, if they have the option to familiarize

---

[5] While the term "data" refers to the original data itself, "information" is understood as the product of the analysis of data.

[6] *See also* Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work and Think (2013) (giving examples of the possibilities offered by big data).

[7] *See, e.g.*, Yannis Bakos et al., Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts 1, 3, 26 (N.Y.U. L. & Econ. Working Papers, Paper No. 195, 2009) (this study investigated the browsing habits of 45,091 households regarding 66 online software companies and showed that only in 0.05 percent of the 120,545 visits to the sites the license agreements were clicked on for at least one second and that an average stay on the license agreement site of 47.7 seconds was not sufficient to even read the average 2,277 words. During 5,509 visits that entered a secure session (which indicates the formation of a contract), only in 0.11 percent of the cases the terms of contract were accessed); see also John Brownlee, GameStation EULA collects 7,500 souls from unsuspecting customers, Geek (Apr. 16, 2010), http://www.geek.com/games/gamestation-eula-collects-7500-souls-from-unsuspecting-customers-1194091/ (this software company on April 1, 2010 added the following clause to their standard terms of contract: "By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non transferable option to claim, for now and for ever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it,

themselves with all important information regarding the disclosure and, e.g. out of lack of time or laziness, do not use this chance, from a legal perspective such disclosure is to be considered voluntary.

By contrast, self-disclosure is involuntary if users: a) are physically forced to disclose (a rather rare scenario that the paper will not pay further attention to); b) lack the necessary capacity to understand the decision (as, for example, minors or mentally ill people might);[8] or c) encounter themselves in situations where the freedom of decision is severely restricted. The latter may be the case if persons lack any bargaining power, but have a great need to receive a good or service.[9]

In all other situations, both explicit and implicit self-disclosure are to be considered voluntary.[10] In specific cases, especially the implicit

---

within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorized minions. We reserve the right to serve such notice in 6 (six) foot high letters of fire, however we can accept no liability for any loss or damage caused by such an act. If you a) do not believe you have an immortal soul, b) have already given it to another party, or c) do not wish to grant Us such a license, please click the link below to nullify this subclause and proceed with your transaction." Though the opt-out-option was optically highlighted and though an opt-out was awarded with a five-Pound-voucher, 88 percent of the users (ca. 7,500 users) accepted the clause).

[8] *See generally* Bundesverfassungsgericht Entscheidungen [BVerfGE] [Federal Constitutional Court Cases] Feb. 10, 1960, 10, 302 (322) (Ger.); BVerfGE July 18, 1967, 22, 180 (219) (Ger.); BVerfGE July 10, 1981, 58, 208 (224) (Ger.); Bundesverwaltungsgericht [BVerwG] [Federal Administrative Court], Feb. 14, 1989, NJW 1989 (2960-2961) (Ger.); Bayerischer Verfassungsgerichtshof [BayVerfGH] [Bavarian Constitutional Court], NJW 1989, 1790 (1790-1791) (Ger.).

[9] S*ee* BVerfG, Oct. 23, 2006, MMR 2007, 93 (93) (Ger.); BVerfG, RDG 2013, (230 et seq.) (Ger.); Entscheidungen des Bundesgerichtshofs in Zivilsachen [BGHZ] [Federal Court of Justice Civil Cases] July 16, 2008, 177, 253 (Ger.) (these cases are further examples for restricting decisional freedom or rendering the validity of consent).

[10] *See, e.g.*, German Genetic Diagnosis Act [GGDA], § 18, para. 1, sentence 2 (if the self-disclose is to be considered involuntarily, governments clearly have the power, and in Germany even the duty, to protect citizens from making such involuntary decisions. The GGDA includes regulations that prohibit data collectors from receiving certain sensitive data, like genetic data); German Federal Data Protection Act [GFDPA], § 28, para. 3(b) (prohibits rendering consent invalid); German Federal Data Protection Act [GFDPA], § 28(a), para. 2, sentence 4 (also prohibits rendering consent invalid) (Ger.); European Union General Data Protection Regulation [EUGDPR], Jan. 25, 2012 at art. 7, § 4, (original draft declared consent to be invalid in case of a "significant imbalance between the position of the data subject and the controller") (Ger.); Employee Polygraph Protection Act, 29 U.S.C. § 2002 (1988) (which prohibits employers (with a few exceptions) to use, accept, refer to, or inquire concerning the results of any lie detector test an employee or prospective employee has undertaken) (in determining whether disclosure is involuntary, for practical reasons and to achieve legal certainty, governments may use simplifying categories (age/certain dangerous situations) as long as they are reasonable).

ones, German and U.S. law might lead to different assessments as to which acts of self-disclosure are to be regarded as voluntary. In this article, we opt for a broad reading, according to which all acts of self-disclosure, except for the three named exceptions which are seen as voluntary to allow a comprehensive analysis of all potentially relevant legal questions.

B. HARM TO SELF-DEVELOPMENT CAUSED BY ONLINE SELF-DISCLOSURE

A lack of privacy may cause harms to the individuals themselves. Individuals' cognitive processes depend on unbiased and unrestricted access to information and an uninhibited development of ideas. Self-disclosure can harm this process in various ways, which will be analyzed in the following paragraphs.

I. *Effects of Filter Bubbles on the Selection of Information*

The creation of new ideas is based on the available information. The search for information is now in large part conducted online. A 2010 study of the Pew Research Center found that 34 percent of the participants had consumed news online on the day before, while 17 percent had read an online news magazine.[11] Forty-seven percent used search engines at least once a week to retrieve news, while 17 percent did so daily. Additionally, 16 percent regularly used social networks to receive news, while 26 percent sometimes did so. Also, eleven percent used blogs to get news on a regular basis, while 24 percent sometimes did so.[12]

The primary way to access information online is via search engines. The algorithms in search engines aim to recognize correlations between information and thereby optimize the displayed results. According to Professor Christopher Yoo: "It is thus hard to see how to make sense of criticisms that search engine results are 'biased' when bias is the very essence of the enterprise."[13] However,

---

[11] *See Americans Spending More Time Following the News: Ideological News Sources: Who Watches and Why*, THE PEW RESEARCH CENTER FOR THE PEOPLE & THE PRESS 105 (2010), http://www.people-press.org/files/legacy-pdf/652.pdf.

[12] *Id.* at 93, 119.

[13] *See* Christopher Yoo, *Free Speech and the Myth of the Internet as an Unintermediated Experience*, 78 GEO. WASH. L. REV. 697, 708 (2010).

even the very essence of an enterprise must face criticism if it has the potential to cause harm.

Entering a search query and accessing a website can be activities that disclose the users' thoughts.[14] While users are searching for information online, website operators and internet service providers can store the URL of the accessed websites, search engine operators can record the searched items and accessed hits, and email providers can retain email metadata.[15] Similarly the documentation of the search for information creates "intellectual records", which provide a "partial transcript of the operation of a human mind".[16] Among other uses they are put to, these records are analyzed to support or influence users by providing them with personalized content and advertising.

When ranking search engine hits, the algorithms take into consideration personalized factors[17] to estimate which hits are likely to be considered relevant by the users.[18] For users, great importance lies with the content of the first page(s), as the effort required to access

---

[14] *See* Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 CHI. L. REV. 261, 272 (2008) (pointing out that "Internet searches raise significant privacy concerns because they can represent the most intimate and spontaneous of one's online activities. An internet search reflects unvarnished thoughts and ponderings rather than one's more considered communications or transactions."); LAWRENCE LESSIG, CODE: VERSION 2.0 204 (2006) (summarizing that "[c]uriosity is monitored, producing a searchable database of the curious. [...] Before search engines, no one had any records of curiosity; there was no list of questions asked.").

[15] *See* Kurt Opsahl, *Why Metadata Matters*, ELECTRONIC FRONTIER FOUNDATION (June 7, 2013), https://www.eff.org/deeplinks/2013/06/why-metadata-matters ("They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don't know what you talked about. They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret. They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed. They know you called a gynecologist, spoke for a half hour, and then called the local Planned Parenthood's number later that day. But nobody knows what you spoke about.").

[16] Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 436 (2008).

[17] *See, e.g.*, Martin Feuz et al., *Personal Web Searching in the Age of Semantic Capitalism: Diagnosing the Mechanisms of Personalization*, 16 FIRST MONDAY (2011) (this personalized search also takes into account statistical data about age groups, location, financial situation, etc.; the displayed search results are even modified in areas where there is no prior search history of the individual user).

[18] *See* ELI PARISER, FILTER BUBBLE 10 (2012) (search engine personalization may even influence the total number of displayed results; in this example, two users searching the same term in Google received 180 million and 139 million hits respectively).

results further down the line means those results can be regarded as de facto non existent. For example, when searching Google for "BP", some users might primarily see information about investment possibilities at the oil company BP, while others will be lead to information about the oil tragedy caused by BP.[19] Similarly, the algorithms of social networks decide whom to show which information at what position.[20] If left-wing oriented users do not see posts of their conservative friends and vice versa,[21] information about alarming drawbacks may not be noticed or situations may appear distorted, as users may only learn about the arguments of one side.

Instead of coming to know other opinions, users may get caught in "feedback loops"[22] which create "echo chambers of thought"[23] and isolate them from opposing ideas. A "filter bubble" is created,[24] and users are manipulated by algorithms. Professor Lawrence Lessig notes: "The observing will affect the observed. The system watches what you do; it fits you into a pattern; the pattern is fed back to you in form of options set by the pattern; the options reinforce the pattern; the cycle begins again".[25]

Such a personalization can be used to enforce political or economic interests. Whereas readers of a left-wing newspaper will be well aware of a political bias within the articles, online users usually are ignorant of the omnipresent pre-selection of sources by algorithms.[26] This lack of transparency in addition to the missing chance to opt-out of personalization leaves users with no way to

---

[19] *Id.* at 10.

[20] *See* Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1913 (2013).

[21] *See* ELI PARISER, FILTER BUBBLE 13 (2012) (describing that this occurred to him).

[22] *See* Cynthia Dwork & Deirdre K. Mulligan, *It's Not Privacy, And It's Not Fair*, 66 STAN. L. REV. 35 (2013).

[23] *See* Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. 41, 44 (2013).

[24] *See* Eli Pariser, *The Filter Bubble*, THE ATLANTIC (Oct. 10 2010), http://www.theatlantic.com/daily-dish/archive/2010/10/the-filter-bubble/181427/ (defining the filter bubble as a "personal ecosystem of information that's been catered by these algorithms to who they think you are"); *see also* ELI PARISER, FILTER BUBBLE 17 (2012); Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1917 (2013).

[25] Lawrence Lessig, Code: Version 2.0 220 (2006).

[26] *See* ELI PARISER, FILTER BUBBLE, *supra* note 18, at 18 (2012).

escape from this interference with their gathering of information. Further research is impeded, as it seems as if all necessary information is received. Eli Pariser gives an allegory: If your plate is filled with delicious information, why would you want to look further?[27] Users thus can be subtly steered in one direction and, thereby, be hindered in forming an autonomous opinion.

II. *Inhibiting Effects on the Access to Information*

In addition to being imperceptibly withheld from accessing information that does not suit their profiles, users might abstain completely from accessing certain information to avoid negative consequences.

Until recently, information that was once disclosed was likely to be forgotten as time passed by. Though it may have been stored somewhere in a newspaper archive or a book, it was practically obscure,[28] as described in a concurring opinion in United States v. Jones: "In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken."[29] Due to technical developments, vast amounts of data are now collected and processed by countless parties and are available and accessible for an unlimited period of time. Thereby, such "dataveillance"[30] creates an impression of being watched similar to traditional physical forms of surveillance.[31]

Humans are embedded in their social environment and therefore eager to leave positive impressions on everyone who observes them. People might aim at appearing likeable, intelligent, smart and foresighted, and at hiding mistakes and changes of mind. Thus, the

---

[27] *Id.* at 102.

[28] *See* United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762 (1989) (acknowledging a privacy interest in maintaining such practical obscurity).

[29] United States v. Jones, 132 S. Ct. 945, 963 (2012).

[30] *See* Roger Clarke, *Information Technology and Dataveillance*, ROGERCLARK.COM (Nov. 1987), http://www.rogerclarke.com/DV/CACM88.html (introducing the term "dataveillance").

[31] *See* James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 9 (2003); Daniel J. Solove, "*I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 765 (2007).

impression of being watched can alter the individuals' behavior, as Professor Christopher Slobogin notes: "Imagine now being watched by an officer [...] every time you walk through certain streets. Say you want to run (to catch a bus, for a brief bit of exercise or just for the hell of it). Will you? Or assume you want to obscure your face (because of the wind or a desire to avoid being seen by an officious acquaintance)? How about hanging out on the street corner (waiting for friends or because you have nothing else to do)? In all of these scenarios, you will probably feel and perhaps act differently than when the officer is not there. Perhaps your hesitancy comes from uncertainty as to the officer's likely reaction or simply from a desire to appear completely law-abiding; the important point is that it exists."[32]

As users cannot foresee who is watching them and what activities the watchers might (today or any day in the future) perceive as negative, it is likely that users will limit themselves to the least-risky behavior and "conformistically" stick with the mainstream.[33] Regardless of the question whether users in fact are watched at a given time, the mere fear of being watched can alter their behavior as it does with the panopticon's prisoners.

Such a self-censorship as a result of the fear of being watched is well-recognized by the German Federal Constitutional Court, the Bundesverfassungsgericht.[34] The court based the necessity to develop a right to informational self-determination precisely on these findings: "If citizens cannot oversee and control which or even what kind of information about them is openly accessible in their social environment, and if they cannot even appraise the knowledge of possible communication partners, they may be inhibited in making use of their freedom. If citizens are unsure whether dissenting behavior is noticed and information is being permanently stored, used and passed on, they will try to avoid dissenting behavior so as not to

---

[32] *See* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 241 (2002).

[33] *See also* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1216 (1998); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 108-109 (2009).

[34] *See* BVerfGE, June 11, 1958, 7, 377 (378) (Ger.); BVerfGE, July 14, 1999, 100, 313 (381) (Ger.); BVerfGE, Mar. 3, 2004, 109, 279 (354) (Ger.); BVerfGE, Feb. 27, 2008, 120, 274 (323) (Ger.); BVerwG, Aug. 22, 2006, NJW 2007, 351 (354) (Ger.).

attract attention. They may even abstain from making use of their basic and human rights."[35]

If users are made uncomfortable by the thought that someone could come to know that they accessed certain online resources, the described self-censorship might inhibit their access to controversial resources. A 2013 study asked 528 U.S.-journalists whether fear of online surveillance had changed their research behavior. Sixteen percent stated that this fear had actually made them not search for certain terms in search engines or not access certain websites, twelve percent said they had considered to refrain from these actions.[36]

A lack of informational privacy may thus constrain the users' access to information outside the mainstream.

III. *Inhibiting Effects on the Creation of Ideas*

Besides the non-biased access to resources and the possibility to use them without fear, the possibility to think without being watched and to discuss with trusted persons is crucial to develop new ideas.

The creation of ideas depends on the individual's freedom to consider and reject a variety of ways (including unorthodox ones), and to change opinion until the final product is ready to be shared with the environment.[37]

Both the process of thinking and the exchange with trusted persons are to a large degree mediated by online services. Documents are stored in the cloud, ideas are noted in online diaries, and thoughts get exchanged via emails, chats or blogs. Society faces a "migration of thought [...] to the electronic environment".[38]

A feeling of being watched during these processes hinders the creation of ideas. As Professor Paul M. Schwartz notes, "perfected surveillance of naked thought's digital expression short-circuits the

---

[35] BVerfGE, Dec. 15, 1983, 65, 1 (42) (Ger.); Gerrit Hornung & Christoph Schnabel, *Data protection in Germany I: The population census decision and the right to informational self-determination*, 25 COMPUTER L. & SECURITY REV. 84, 85 (2009).

[36] *See* FDR Group, *The Impact of U.S. Government Surveillance on Writers: Findings from a Survey of PEN Membership*, PEN AMERICA (Oct. 31, 2013), http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.

[37] *See also* Stephen J. Schulhofer, More Essential Than Ever: The Fourth Amendment in the Twenty First Century 12 (Geoffrey R. Stone, ed., 2012).

[38] Richards, *supra* note 16, at 444.

individual's own process of decision-making."[39] To avoid negative consequences, self-censorship may therefore limit ideas to conformist views, the well-recognized and the mainstream.[40] Thus, individuals may turn "boring".[41] Additionally, they might refrain from sharing controversial ideas with trusted persons to avoid negative consequences for the latter.

Thus, Professor Julie E. Cohen calls for "informational autonomy",[42] and Professor Daniel J. Solove calls for "free zones for individuals to flourish".[43] Furthermore, one needs to be able to discuss preliminary ideas with trusted persons to receive feedback, and be able to keep, change or withdraw the idea accordingly. Professor Neil M. Richards describes an "infant industries' rationale, serving to nurture and shield new ideas from social disapproval before they are ready to be disclosed."[44] To avoid thoughts to be inhibited, he calls for the protection of intellectual privacy, claiming that "the protection of records of our intellectual activities [...] safeguards the integrity of our intellectual activities by shielding them from the unwanted gaze or interference of others."[45]

IV. *Conclusion*

A biased or inhibited access to resources as well as a restricted ability to freely evolve ideas hinders individuals from developing their personality. Conformist ideas hence lead to conformist behavior.

---

[39] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1656 (1999).

[40] *See also* Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 STAN. L. REV. 1373, 1425 (2000); Lilian Mitrou, The impact of communications data retention on fundamental rights and democracy – the case of the EU Data Retention Directive, in SURVEILLANCE AND DEMOCRACY 133 (Kevin D. Haggerty & Minas Samatas, eds., 2010).

[41] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1948 (2013).

[42] *See* Cohen, *supra* note 40, at 1425.

[43] *See* Solove, *supra* note 31, at 762.

[44] *See* Richards, *supra* note 16, at 404.

[45] *Id.* at 387; *see also* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 448 (1980); Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 576 (2003) (describing intellectual privacy as "the extent of 'breathing space' both metaphorical and physical, available for intellectual activity").

Additionally, the potential for economic success through new ideas and business models gets impaired.

Therefore, even voluntary disclosure, despite all its obvious advantages, can cause great harm to the individuals themselves.

C. TWO PATERNALISTIC APPROACHES TO PREVENT ONLINE SELF-DISCLOSURE

To fight the described risks caused by excessive self-disclosure, governments may wish to completely prevent[46] certain disclosures.

In doing so, they may of course focus only on assisting users to manage their own privacy. As these measures do not infringe upon the users' rights, governments may always apply them. Under German law, the government is even constitutionally obliged to help users to protect themselves.[47] This idea of privacy self-management[48] is based on empowering users to make their own decision about self-disclosure based on their own cost-benefit-analysis. Tools to achieve this are traditionally and primarily based on increasing transparency by notice, especially through information requirements or privacy policies which inform users about the collection and use of their data. Other examples would be the concepts of privacy by design, including privacy-enhancing technologies which integrate privacy protection

---

[46] European Union General Data Protection Regulation [EUGDPR], Jan. 25, 2012, art. 17 (describing that another, less invasive but also less effective, option would be to soften the effects of self-disclosure, e.g., by enacting strict rules on data security, or by strengthening the users' rights to correct or delete certain information (an example would be a "right to be forgotten")) (Ger.); *see also* Jeffrey Rosen, *The Right to be Forgotten*, 64 STAN. L. REV. 88, 88 (2012) (elaborating on a critical U.S. perspective).

[47] Grundgesetz [GG] [Basic Law], Art. 1, para. 1, Art. 2, para 1, *translation at* http://www.gesetze-im-internet.de/englisch_gg/index.html (detailing a duty to protect the users' right to informational self-determination) (Ger.); *see* BVerwG Oct. 23, 2006, MMR 2007, 93 (93) (to fulfill a duty to protect users' right to informational self-determination, the German government must set a legal framework that allows users to decide in a self-determined way whether to disclose their data. This case lays out the Bundesverfassungsgericht reasons that the government has to ensure that individuals can participate in communication processes self-determinedly by empowering them to undertake effective informational self-protection) (Ger.).

[48] *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013) (also uses the term "privacy self-management").

into a service or process.[49] Further, privacy education can assist users in making informed choices according to their preferences.

Governments can promote such privacy self-management by providing the necessary infrastructure, incentivizing or supporting its development, ensuring its legal enforceability, or offering a privacy audit service.[50] Professor Gregory Mitchell describes such interventions as "liberty-focused paternalis[m]", which prefers individual freedom over objective welfare, and is "happy to trust free individuals to make their own welfare decisions and let them live with the consequences" (thereby rejecting the idea of libertarian paternalism, to be discussed below).[51] Government measures to promote privacy self-management are characterized by the governments' primary goal to empower individuals to make their own decision, without aiming to steer users in a specific direction.

This paper is concerned with a more effective – though more difficult to justify – path: to prevent certain disclosures by paternalistic measures. When doing so, governments may pursue two different ways. Governments may pursue either a traditional paternalistic approach of compelling protection, or the more modern libertarian-paternalistic approach of nudging.

I. *Compelled Protection*

The most effective way to prevent self-disclosure is to compel users toward not disclosing certain aspects of their informational privacy. The government decides which disclosures generally bear more risks than benefits and prevents such disclosures. This can be accomplished in two different ways, which both de facto result in less self-disclosure:

Firstly, government could forbid users to disclose their data and thereby render online self-disclosure impossible.

---

[49] *See Enabling smarter privacy tools for the web*, PLATFORM FOR PRIVACY PREFERENCES PROJECT (Nov. 20, 2007) (examples include anonymous/pseudonymous services, encryption, a consistent and legally binding do-not-track-standard, tools to block certain scripts or cookies, proxy-servers, or P3P-agents that compare the users' privacy preferences with a website's machine readable privacy policy to enable users to make an informed decision about whether to access the website or not).

[50] *See* German Federal Data Protection Act [GFDPA] § 9a (a basis for the implementation of such an audit in Germany) (Ger.).

[51] *See* Gregory Mitchell, *Libertarian Paternalism Is an Oxymoron*, FSU College of Law, Law and Economics Paper No. 05-02 at 31.

Secondly, data collectors could be prohibited from collecting or using revealed data, even if users would like to share them. To make certain data collection/use impossible, data collectors may additionally be forced to change their codes[52] in ways that disclosure would be technically impossible.

An example for preventing explicit self-disclosure would be to prohibit the collection or use of sensitive data such as genetic data. Implicit disclosure could be prevented by prohibiting certain kinds of browser tracking (even with users' consent). The data collectors would then be forced to accordingly change their codes.

Compelling protection has been the traditional approach of governments all around the world to prevent all sorts of dangers their citizens face.

II. *Nudges*

A second way that currently receives great attention from scholars is to prevent users from self-disclosure by using nudges (see E III for the libertarian paternalistic justification of nudges).[53]

Findings of behavioral psychology show that users are predictably irrational.[54] When facing complicated situations, rational decisions are replaced by simplifying models, approximation strategies or heuristics.[55] Scholars suggest measures that would prevent or limit irrational decisions (debiasing through law).[56] An example would be a legal command to use so-called libertarian paternalistic measures

---

[52] According to Professor Lawrence Lessig, the regulation of cyberspace is governed by code (understood as hardware and software), the architecture of cyberspace, *see* Lessig, *Code supra* note 14, at 5 et seq. While he relies on the market directing this code, for the purpose of this paper, regulation of code by law is considered a way of compelled protection.

[53] *See* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH AND HAPPINESS (2008).

[54] *See* Dan Ariely, Predictably Irrational: The Hidden Forces That Shape Our Decisions (2010).

[55] *See* Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy? in* DIGITAL PRIVACY: THEORY TECHNOLOGIES AND PRACTICES 364, 369 (Alessandro Acquisti ed., 2008).

[56] *See* Christine Jolls, *Rationality and Consent in Privacy Law*, at 54 et seq. (2010), *available at* http://isites.harvard.edu/fs/docs/icb.topic503720.files/Jolls%203%2017.pdf.

such as nudges.[57] Such tools are paternalistic because the government decides what is best for the citizens. Thereby they are treated as an object of government decision-making. Simultaneously, the measures are supposed to be somewhat libertarian, as citizens are left with the possibility to act differently from what they are nudged to do.[58] Knowledge about irrationalities in decision-making can be used to design choice architectures for users in a way they are likely to decide as the architect intends them to decide.[59] There is a wide variety of possible privacy nudges.

A very basic example is the use of privacy-enhancing defaults. People are more likely to keep a status quo than to initiate changes.[60] Taking this into consideration, the use of privacy by default could lead to a substantially lower degree of self-disclosure.

Also, providing users with feedback before or after committing mistakes can decrease the probability of such errors. A non-representative study initially surveyed that users often regret having made their Facebook posts available to an overly large audience. To prevent them from committing those mistakes, before being able to post or comment on Facebook, users were confronted with five pictures of other users who would be able to view the post.[61] The pre-study further indicated that users frequently regret having posted excessively emotional posts or comments. To impede them from doing so, before being able to send an emotional post or comment the users were shown a note. For example, "Other people might perceive your

---

[57] Scholars have suggested various terms, *see* Rhys Jones, Jessica Pykett & Mark Whitehead, *Governing Temptation: Changing Behaviour in an Age of Libertarian Paternalism*, 35 PROGRESS IN HUMAN GEOGRAPHY 483 (2011) ("behaviour change policies"); Mario J. Rizzo & Douglas G. Whitman, *Little Brother is Watching You: New Paternalism on the Slippery Slopes,* 51 ARIZ. L. REV. 685, 685 (2009) ("new paternalism"), and Christine Jolls, Cass R. Sunstein & Richard H. Thaler, *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471, 1541 et seq. (1998) ("anti-antipaternalism").

[58] *See* Cass R. Sunstein, *The Storrs Lectures: Behaviour Economics and Paternalism*, 122 YALE L.J. 1826, 1835 (2013).

[59] *See* Thaler & Sunstein, *Nudge*, *supra* note 53, at 89 et seq.

[60] *See* Cass R. Sunstein & Richard H. Thaler, *Libertarian Paternalism is Not an Oxymoron*, 70 U. CHI. L. REV. 1159, 1174 et seq. (2003).

[61] *See* Yang Wang et al., *From Facebook Regrets to Facebook Privacy Nudges*, 74 OHIO ST. L.J. 1307, 1321 (2013).

post as negative".[62] Both models induced users to not publish the post, change the audience, or modify their privacy settings.

Additionally, a variety of other incentives can be used to trigger privacy-enhancing behavior. People suffer from optimism-bias and thus systematically overrate the probability of the occurrence of positive events while underestimating the one of negative events. For example, in the context of social networks users know about privacy problems, but expect not to be affected by them.[63] Moreover, if a harm is hard to imagine, like identity theft, people underestimate the probability of its occurrence.[64] These predictable irrationalities can be used to alter behavior by drawing users' attention to certain factors. Users could be prevented from implicitly compromising their informational privacy on privacy-invading websites if those websites had to display an avatar which follows the user. With one click, users could either fade out the avatar or opt-out of the tracking.[65]

Moreover, the way different alternatives are framed affects the decisions that are made by users. The option "Click here for continuous surveillance" will appear less attractive to the user than "Click here for more relevant advertising".[66] As the design of a website can influence the decision whether to trust the website or not, changing the design while leaving the content unchanged can be used to prevent users from excessive self-disclosure.

Another privacy-enhancing nudge could be to increase transaction costs. For example, while the revealing of most kinds of personal data

---

[62] *Id.* at 1322. Nevertheless, follow-up interviews showed that participants disliked the emotional feedback tool, *see id.* at 1327 et. seq. So far, scholars seem to have paid little attention to the fact that many privacy-enhancing nudges imply privacy invading technologies, such as analyzing the content of posts to estimate if it is emotional.

[63] *See* Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, at 13-14 (2006), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf.

[64] *See* Acquisti & Grossklags, *supra* note 55.

[65] Professor Ryan Calo describes this tool as part of his concept of "visceral notice." Other than content-neutral notice, the tool seems more appropriately considered as using behavioral economic insights to change behavior and therefore in this paper is listed as a nudge rather than a notice, *but see* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1040 (2012).

[66] *See* Frederik Zuiderveen Borgesius, Consent to Behavioural Targeting in European Law: What are the Policy Implications to Insights from Behavioural Economics?, at 51 (draft for the Privacy Law Scholars Conference (Berkeley July 2013)).

would only require one click, the disclosure of sensitive data could afford either several clicks or even signing and mailing a consent form.[67] Also, a mandatory waiting period before a taken decision comes into effect could limit disclosure. Based on pre-study findings that users frequently regret rushed Facebook posts, the above mentioned non-representative study tested a ten-second waiting period before a post or comment would be published.[68] The feature, when given, allowed users to wait, edit the post, delete the post or skip the waiting. Several users thus edited posts or refrained from publishing a post at all.[69]

The line between promotion of privacy self-management and nudges sometimes turns blurry. However, it seems preferable to differentiate measures that do not aim at altering the decision (promotion of privacy self-management) and those that serve to modify the decision (nudges). Such a distinction proves especially necessary as the law treats both kinds of measures differently.[70]

D. GOVERNMENTAL DUTY TO PATERNALISTICALLY PREVENT ONLINE SELF-DISCLOSURE

In the face of the described harms that self-disclosure can cause,[71] both the German and the U.S. government could be thought to be constitutionally obliged to use compelled protection or nudges to prevent competent adult users from certain acts of voluntary self-disclosure to safeguard the endangered constitutional rights, i.e. the users' interests in their free access to information and the unhindered development of their personalities.

---

[67] *See id.* at 56.

[68] *See* Wang et al., *supra* note 61, at 1321-1322.

[69] *See id.* at 1328-1329.

[70] For the legal situation in the United States, *see, e.g.*, Zauderer v. Office of Disciplinary Counsel of Supreme Court of Ohio, 471 U.S. 626, 651 (1985) (a duty to convey purely factual and uncontroversial information faces a low scrutiny), *but see* R.J. Reynolds Tobacco Co. v. Food and Drug Admin., 696 F.3d 1205 (D.C. Cir. 2012) (graphic warnings on cigarette packages face intermediate scrutiny).

[71] See B.

I. *Analysis: German Constitutional Law*

German basic rights are not limited to the function of protecting individuals against the government, but also create a so called objective order of values that serves as a constitutional basis for all areas of the law ("objektive Wertordnung").[72] Therefore, the law as such (including civil law) has to be interpreted in the light of the basic rights. Against this background, the doctrine of a duty to protect has been developed. If private actors threaten the basic rights of individuals who cannot defend themselves the individuals' basic rights may oblige the government to protect them from the other private actors ("Schutzpflicht").[73]

When choosing the desired level of protection and the means used to achieve this protection, the government can act at its own discretion ("Gestaltungsspielraum").[74] However, it must not refrain from taking any action or take evidently insufficient measures ("Untermaßverbot").[75]

As self-disclosure may cause harms to the development of the users' personality, the government could be obliged to prevent users from excessive self-disclosure in order to protect them.

In a few cases, courts have held that the government was obliged to protect citizens from harms caused by their own voluntary conduct. Above all, those cases involved the protection of the citizens' human dignity.[76] It was held to be endangered by a woman dancing in a peep

---

[72] *See* BVerfGE, Jan. 15, 1958, 7, 198 (205) (Ger.).

[73] *See* BVerfGE, Feb. 25, 1975, 39, 1 (42) (protection of the unborn child against abortion) (Ger.); BVerfGE, May 28, 1993, 88, 203 (252) (same) (Ger.); BVerfGE, Oct. 16, 1977, 46, 160 (164-165) (protection against terrorism) (Ger.); BVerfGE, Aug. 1, 1978,49, 24 (53 et seq.) (same) (Ger.); BVerwG Dec. 20, 1979, 53, 30 (Ger.); BVerfGE, Aug. 8, 1978, 49, 89 (142) (protection against technical and environment dangers) (Ger.); BVerfGE, Dec. 20, 1979, 53, 30 (57) (same) (Ger.); BVerfGE, Jan. 14, 1981, 56, 54 (73, 78) (same) (Ger.); BVerfGE, Oct. 29, 1987, 77, 170 (214) (same) (Ger.); BVerfGE, Nov. 30, 1988, 79, 174 (201-202) (same) (Ger.).

[74] *See* BVerfGE, Oct. 29, 1987, 77, 170 (215) (Ger.).

[75] *See* BVerfGE, May 28, 1993, 88, 203 (254 et seq.) (Ger.).

[76] *See* Art. 1 para. 1 Basic Law, *translation available at* http://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0015 (Ger.).

show, and[77] by a growth-restricted person who wanted to be tossed as part of a commercial dwarf tossing game ("Zwergenwerfen").[78]

However, paternalistic protections of human dignity (and even more regarding other legal interests) have been widely criticized.[79] In more recent cases, the Bundesverfassungsgericht did not acknowledge duties to protect competent adult individuals from menaces caused by themselves, but held that basic rights are only meaningfully protected if they allow individuals to endanger themselves[80], to reject treatment of curable diseases,[81] etc.

Similarly, the Bundesverfassungsgericht held government intervention with the sole aim of improving individuals to be unacceptable, for example when the court rejected government measures to place competent adult persons in mental hospitals with the sole goal of making them (in the eyes of government) a better person.[82]

Informational privacy is not necessarily protected by the users' human dignity, and thus the courts' widely criticized rulings on a government duty to protect human dignity may only in few instances (such as disclosing especially intimate personal data) indicate a possibility to protect users against themselves. But even in these cases a duty to protect has, in accordance with the views of the overwhelming majority of scholars, to be rejected. A society such as the German one, which even no longer prohibits prostitution a fortiori certainly does not acknowledge a government duty to limit online self-disclosure of intimate data.

Furthermore, the idea of protecting persons from their own voluntary actions contradicts their freedom to informational self-

---

[77] *See* BVerwGE, Dec 15, 1981, 64, 274 (277 et seq.). (Ger.) The decision has widely been rejected in scholarship, *see, e.g.*, Wolfgang Schatzschneider, 'Rechtsordnung und Prostitution' NJW 1985, 2793, 2796-2797 (Ger.).

[78] *See* Verwaltungsgericht Neustadt [Administrative Court Neustadt] May 21, 1992, NVwZ 1993, 98, 99 (Ger.).

[79] *See, e.g.*, Eckart Klein, 'Grundrechtliche Schutzpflicht des Staates' NJW 1989, 1633, 1640 (Ger.).

[80] *See* BVerwG, Nov. 8, 1999, NJW 1999, 3399, 3401 (Ger.).

[81] *See* BVerfGE, Oct. 7, 1981, 58, 208 (226).

[82] *See* BVerfGE, July 18, 1967, 22, 180 (219 et seq.) (Ger.); BVerfGE, Dec. 15, 1970, 30, 47 (53) (Ger.).

determination. Hence, there is no duty to coerce privacy on competent adult users to protect themselves.

II. *Analysis: U.S. Constitutional Law*

Except for the protection against slavery,[83] U.S. constitutional law does not include any government duties to protect. Such duties were rejected in cases where the government knew about the severe abuse of a four-year-old child,[84] or about the kidnapping of three kids who ultimately died, but failed to act on that knowledge.[85] A duty for government officials to help the victims of accidents was declined because "[t]he men who wrote the Bill of Rights were not concerned that government might do too little for the people but that it might do too much to them."[86]

Constitutional protection only arises in case of state action.[87] Though various online services serve a tremendously important role in the everyday life of citizens, courts have held that internet service providers,[88] search engines[89] and Yahoo! email groups[90] cannot be considered state actors.

Professor Jeffrey Rosen recently called for a "constitutional amendment to prohibit unreasonable searches and seizures of our persons and electronic effects, whether by the government or by private corporations like Google and AT&T."[91] However, this

---

[83] *See* Civil Rights Cases, 109 U.S. 3, 21 (1883).

[84] *See* DeShaney v. Winnebago Cnty. Dep't of Social Servs., 489 U.S. 189, 196 (1989).

[85] *See* Town of Castle Rock, Colo. v. Gonzales, 545 U.S. 748, 768 (2005).

[86] *See* Jackson v. City of Joliet, 715 F.2d 1200, 1203 (7th Cir. 1983).

[87] *See* Civil Rights Cases, 109 U.S. at 11, 13 ("It is State action of a particular character that is prohibited. Individual invasion of individual rights is not the subject matter.").

[88] *See* Green v. Am. Online (AOL), 318 F.3d 465, 472 (3d Cir. 2003); Howard v. Am. Online Inc., 208 F.3d 741, 754 (9th Cir. 2000); Noah v. AOL Time Warner, Inc., 261 F. Supp. 2d 532, 546 (E.D. Va. 2003); Cyber Promotions, Inc. v. Am. Online, Inc., 948 F.Supp. 436, 443 (E.D. Pa. 1996).

[89] *See* Langdon v. Google, Inc., 474 F. Supp. 2d 622, 631-632 (D. Del. 2007).

[90] *See* Murawski v. Pataki, 514 F. Supp. 2d 577, 588 (S.D.N.Y. 2007).

[91] *See* Jeffrey Rosen, *Madison's Privacy Blind Spot*, N.Y. TIMES, Jan. 18, 2014,, *available at* http://www.nytimes.com/2014/01/19/opinion/sunday/madisons-privacy-blind-spot.html?_r=0 ("[C]ontinuously tracking my location, whether by the government or

interesting proposal has been without major consequences so far. Constitutional privacy protection in the United States thus is limited to repel government intervention – with the exception of the California Constitution, which provides privacy protection also against private actors.[92]

III. *Comparison*

As a basic principle, German and U.S. constitutional law follow opposing approaches regarding a government duty to protect.

Basic German rights can establish governmental duties to protect citizens against private action. By contrast, U.S. law does not recognize any duty to interfere with private relationships.[93]

However, in both legal systems there is no governmental duty to coerce online privacy. Though the German constitution in general acknowledges duties to protect, no duty to coerce or nudge competent

---

AT&T, is an affront to my dignity. When every step I take on- and off-line is recorded, so an algorithm can predict if I am a potential terrorist or a potential customer, I am being objectified and stereotyped, rather than treated as an individual, worthy of equal concern and respect.").

[92] *See* Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 644 (Cal. 1994); see also Wilkinson v. Times Mirror Corp., 215 Cal. App. 3d 1034, 1043 (Cal. App. 1st Dist. 1989) ("Common experience with the ever-increasing use of computers in contemporary society confirms that the amendment was needed and intended to safeguard individual privacy from intrusion by both private and governmental action. That common experience makes it only too evident that personal privacy is threatened by the information-gathering capabilities and activities not just of government, but of private business as well. If the right of privacy is to exist as more than a memory or a dream, the power of both public and private institutions to collect and preserve data about individual citizens must be subject to constitutional control.").

[93] Several scholars have conducted comparative analysis between the two systems, all agreeing on the finding that the U.S. Constitution cannot be read to include duties to protect, *see* Thomas Giegerich, *Privatwirkung der Grundrechte in den U.S.A: Die State Action Doctrine des U.S. Supreme Courts und die Bürgerrechtsgesetzgebung des Bundes* (Springer-Verlag 1992) at 451 et seq.; Friederike V Lange, *Grundrechtsbindung des Gesetzgebers* (Mohr Siebeck 2010) at 416 et seq.; Philipp Wittmann, *Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die U.S.-amerikanische Bundesverfassung* (Nomos 2014) at 38 et seq., *but see* Stephen Gardbaum, *The Myth and the Reality of American Constitutional Exceptionalism*, 107 MICH. L. REV. 391, 442 et seq. (2009) ("[I]f and to the extent that constitutional rights do have less impact on private actors in the United States than in other countries rejecting direct horizontality, it is neither due to an exceptional, more vertical structural position on the scope of rights nor to how the state action doctrine operates. It is exclusively because of substantive differences in the rights themselves and their interpretation; that is, not because fewer laws are subject to constitutional rights scrutiny but because fewer laws may fail it.").

adult users into not voluntarily disclosing certain data can be derived from those. The U.S. Constitution does not state any governmental duties to protect whatsoever and hence does not establish a duty to coerce (or nudge towards) informational privacy.

E. GOVERNMENTAL POWER TO PATERNALISTICALLY PREVENT ONLINE SELF-DISCLOSURE

As shown above, neither the German nor the U.S. government have the duty to employ coercive or libertarian paternalistic measures to protect their citizens' privacy against voluntary self-disclosure. Indeed, it is even questionable whether they have the power to do so, as these measures may infringe upon the rights of the citizens.

I. *Analysis Regarding German Constitutional Law*

1. *The Need to Justify Any Preventions of Online Self-Disclosure*

Even though self-disclosure can harm individuals, self-endangering behavior falls within the scope of the basic rights. Government measures to prevent such behavior therefore need to be justified.[94] The need for justification is not limited to compelled protection which renders online self-disclosure impossible. It is recognized that constitutional rights may as well be infringed upon by government measures that cause an indirect obstruction. Thus, this paper argues that nudges call for justification whenever they significantly hinder online self-disclosure. While this is certainly the case e.g. for nudges that increase transactions costs, one might argue that privacy-enhancing defaults do not significantly hinder online self-disclosure and therefore do not need to be justified. The question whether a nudge constitutes an indirect factual disturbance and thus needs justification will have to be analyzed by the government in every specific case.

The basic right to informational self-determination ("Recht auf informationelle Selbstbestimmung") is not explicitly mentioned in the Basic Law, but has been developed by the Bundesverfassungsgericht in its famous census decision[95] on the basis of Art. 2 para. 1 (personality right) in conjunction with Art. 1 para. 1 Basic Law

---

[94] *See* BVerwG, Nov. 8, 1999, NJW 1999, 3399, 3401 (Ger.).

[95] *See* BVerfGE, Dec. 15, 1983, 65, 1 (43) (Ger.).

(human dignity).[96] The right to informational self-determination protects against unbounded collection, storage, application, and transmission of personal data and affords individuals the right to decide about the disclosure and processing of their personal data.[97] Any government action that limits the users' rights to decide themselves about the disclosure and processing of their personal data infringes upon this right. It is contended whether the right also protects against inhibiting effects that are caused by the mere fear of being under surveillance, thereby granting protection against negative feelings. Recent judgments by the Bundesverfassungsgericht seem to favor such a broad reading.[98]

As individuals are embedded in their social environment and depend on communication with others, the right to informational self-determination cannot create limitless protection.[99] It can be constrained if outbalanced by a public interest,[100] i.e. if there is a statute which aims at a legitimate purpose and does not disproportionally restrict the right in order to reach the purpose. Therefore, a measure is only proportionate if it is suitable ("Geeignetheit"), necessary ("Erforderlichkeit"), and appropriate to reach the goal ("Angemessenheit").[101]

Government action which interferes with the right to informational self-determination is only constitutional if justified. State measures to compel privacy protection or nudge users into disclosing less, even for the sake of protecting individuals, therefore have to be justified if they significantly hinder online self-disclosure.

---

[96] Art. 2 para. 1 Basic Law, *translation available at* http://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0015.

[97] *See* BVerfGE, Dec. 15, 1983, 65, 1 (43) (Ger.).

[98] *See* BVerfGE, Apr. 12, 2005, 113, 29 (46-47) (Ger.); BVerfGE, Mar. 2, 2006, 115, 166 (188) (Ger.); BVerfGE, Mar 11, 2008, 120, 378 (402) (Ger.).

[99] *See* BVerfGE, Dec. 15, 1983, 65, 1 (44) (Ger.).

[100] *See* BVerfGE, Dec. 1565, 1983, 1 (44) (Ger.).

[101] *See, e.g.*, BVerfGE, Apr. 7, 1964, 17, 306 (314) (Ger.).

2. *Are the Measures Justified?*

It has been demonstrated that there is no duty to prevent users from voluntarily disclosing data (see D). A government intervention to do so has to be justified by an outbalancing legitimate interest.

One could argue that the protection of competent adult users against the harms caused by their own self-disclosure could itself serve as an outbalancing legitimate interest: in very few instances, protecting persons against harms caused by their own voluntary behavior has been regarded as such an outbalancing interest. The Bundesverfassungsgericht did so to justify in one case a statute outlawing living organ transplantations between strangers.[102] This decision was however widely criticized by scholars.[103]

The idea of protecting individuals against their own voluntary behavior needs to be rejected. Doing so would pervert the idea of liberty inherent in the basic rights. Basic rights guarantee the freedom to define for oneself how to live, and which moral values to accept. In particular, the right to informational self-determination guarantees the freedom to disclose personal information. Protecting users from the harms caused by their own conduct cannot be regarded a legitimate purpose and therefore cannot outbalance the users' right to informational self-determination.

Hence, the question whether a measure to prevent self-disclosure is constitutional does not depend on how restrictive the measure is. Nudges in most cases are a less restrictive mean than compelled protection, but still lack a legitimate government interest if they only aim at protecting the users against harms caused by their own voluntary conduct. Protecting users from irrational behavior so far has neither by courts nor by scholars been regarded as a legitimate interest which would justify overriding free choice under German law. A discussion similar to the one currently taking place in the United States (see E III) has not evolved.

Therefore, neither compelled protection nor nudges which significantly hinder online self-disclosure can be justified if their only goal is to protect competent adult users against harms caused by themselves.

---

[102] *See* BVerwG, Aug 11, 1999, NJW 1999, 3399, 3400 (Ger.).

[103] *See* Thomas Gutmann, *Gesetzgeberischer Paternalismus ohne Grenzen?*, NJW 1999, 3387, 3387 (Ger.).

II. *Analysis Regarding U.S. Constitutional Law*

Preventing online self-disclosure could protect individuals from harming themselves. However, these measures may infringe upon the users' rights. As pointed out above (see A), users can voluntarily disclose their data online in explicit or implicit ways. Preventing users from disclosing certain data could violate their First Amendment rights and the Due Process Clause.

1. *First Amendment*

The First Amendment forbids federal and state[104] governments from making any law that would abridge the freedom of speech.[105] It protects both the act of speaking and the act of listening and affords individuals the right to publish content online.[106] Only the possession, consumption, sale, or production of obscene material receives no protection,[107] unless limited to the home.[108] Explicit disclosure which does not include obscene material is hence protected by the First Amendment.

Restrictions of the First Amendment face an intermediate scrutiny, if they are limited to time, place, and manner of the

---

[104] The Fourteenth Amendment incorporates the First Amendment, and it is thus applicable also to state governments, *see* Gitlow v. People of State of N.Y., 268 U.S. 652, 666 (1925).

[105] *Id.*

[106] *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844, 853 (1997).

[107] *See* Roth v. United States, 354 U.S. 476, 484-485 (1957) ("All ideas having even the slightest redeeming social importance – unorthodox ideas, controversial ideas, even ideas hateful to the prevailing climate of opinion – have the full protection of the guaranties, unless excludable because they encroach upon the limited area of more important interests. But implicit in the history of the First Amendment is the rejection of obscenity as utterly without redeeming social importance. This rejection for that reason is mirrored in the universal judgment that obscenity should be restrained, reflected in the international agreement of over 50 nations, in the obscenity laws of all of the 48 States, and in the 20 obscenity laws enacted by the Congress from 1842 to 1956.").

[108] *See* Stanley v. Georgia, 394 U.S. 557, 565 (1969) ("Whatever may be the justifications for other statutes regulating obscenity, we do not think they reach into the privacy of one's own home. If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds.").

speech.[109] Such government action therefore can only be justified if it: 1) furthers an important or substantial governmental interest; 2) the governmental interest is unrelated to the suppression of free expression; and 3) if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.[110] The prohibition of speech via a variety of internet technologies was held to be not a time/place/manner-restriction, but a content-based restriction.[111] A fortiori, preventing users from revealing data online, but leaving them with the option to do so offline, is a content-based restriction. Such content-based measures face strict scrutiny, i.e. they can only be justified if the government has a compelling interest and less restrictive alternatives would not be at least as effective in achieving the legitimate purpose. An example for content-based restrictions is a prohibition to publish content online in order to protect minors.[112] Prevention of explicit self-disclosure by compelled protection would infringe upon First Amendment rights.

A moderate alternative to compelling protection would be to use nudges. These could lead to a significant decrease of disclosure. As the following examples show, they nonetheless seem not to face First Amendment scrutiny, though one could argue that they force individuals to listen to ideological government speech. In a Fifth Circuit decision, the court had to decide upon the constitutionality of a statute which forced women before undertaking an abortion to view their fetus in a sonogram, hear the heartbeat, listen to the explanation of the results and the procedure, and wait twenty-four hours afterwards until the abortion could take place. The court refused the argument that such a law would infringe upon the First Amendment rights of the women.[113] It reasoned, "If the sonogram changes a woman's mind about whether to have an abortion [...] that is a function of the combination of her new knowledge and her own 'ideology' [...], not of any 'ideology' inherent in the information she

---

[109] *See* Schneider v. State of N.J., Town of Irvington, 308 U.S. 147 (1939) (prohibition to distribute leaflets in certain locations).

[110] *See* United States v. O'Brien, 391 U.S. 367, 376-377 (1968).

[111] *See* Reno, 521 U.S. at 879-880.

[112] *See id.* at 874.

[113] *See* Texas Med. Providers Performing Abortion Servs. v. Lakey, 667 F.3d 570, 576 (5th Cir. 2012).

has learned about the fetus."[114] Also, the D.C. Circuit Court's decision on images on cigarette packages does not even discuss a possible violation of the smokers' First Amendment rights.[115] A few commentators suggest affording First Amendment protection against measures which aim to alter belief or conduct in an emotional way, but only in the rare cases that the affected persons are granted no option to opt-out.[116] The nudges discussed above (see C) leave choices to opt-out and therefore do not face First Amendment scrutiny.

In contrast, implicit self-disclosure does not receive First Amendment protection at all. The "expression of an idea through activity" has been held to be speech, if an "intent to convey a particularized message was present, and in the surrounding circumstances the likelihood was great that the message would be understood by those who viewed it."[117] Implicit self-disclosure by online activities which lead to the collection of data is not aimed at conveying a particularized message and thus cannot be regarded as speech. Even more, as the users' consent to the collection of their data is not required, users in most occasions might not even be aware of the data collection and surely do not intend to convey messages.

First Amendment protection could also be triggered as implicit self-disclosure allows algorithms to predict which information users would like to access, and thus facilitates their access to information. Unhindered access to information is a prerequisite for free speech and receives First Amendment protection. Limiting implicit disclosure (for example by limiting browser tracking) could make it more complex for users to find information and hence it could be argued that implicit self-disclosure should receive First Amendment protection. However, this paper suggests rejecting such a broad reading. Measures that limit implicit disclosure would: 1) not affect the information users are actually looking for, but only the information they might want to access if they knew they were looking for it; and 2) only require

---

[114] *Id.* at 577.

[115] *See* R.J. Reynolds Tobacco Co. v. Food and Drug Admin., 696 F.3d 1205 (D.C. Cir. 2012).

[116] *See* Peter Ferony, *Constitutional Law – From Goblins to Graveyards: The Problem of Paternalism in Compelled Perception*, 35 W. NEW ENG. L. REV. 205, 225 et seq. (2013) (although he does not dispute the libertarian-paternalistic argument that choice architecture would serve the individual).

[117] Spence v. State of Wash., 418 U.S. 405, 410-411 (1974) (display of an American U.S. flag marked with a peace symbol during the Vietnam war).

additional efforts to find information, not censor anything. The situation seems not to be comparable with actual prior restraints or censorship, and thus should not be awarded First Amendment protection.

2. *Due Process of Law*

Government measures in the realm of privacy have to respect either the high standard of substantive due process of law (strict scrutiny) or only the lower standard of procedural due process of law (rational basis review). Which standard is applicable depends on the respective kind of privacy limitation:

Paradoxically, certain government measures to protect privacy can also infringe upon the users' right to privacy. Courts have recognized a fundamental right to privacy, which protects against federal government intrusion by penumbras surrounding specific guarantees in the Bill of Rights.[118] These rights are applicable to state governments through the incorporation of those guarantees in the Due Process Clause of the Fourteenth Amendment (substantive due process).[119] Fundamental rights are those rights that are "implicit in the concept of ordered liberty",[120] and "deeply rooted in this Nation's history and tradition".[121] Government action which restricts the right to privacy faces strict scrutiny. The right to privacy however mainly protects aspects of decisional privacy,[122] like surgical examinations,[123] the use of contraceptives,[124] the use of contraceptives by non-married

---

[118] *See* Griswold v. Conn., 381 U.S. 479, 484 (1965).

[119] *See* U.S. Const. amend. XIV, § 1-Due Proc ("nor shall any State deprive any person of life, liberty, or property, without due process of law").

[120] Palko v. State of Conn., 302 U.S. 319, 326 (1937), *overruled by* Benton v. Maryland, 395 U.S. 784 (1969).

[121] Moore v. City of E. Cleveland, 431 U.S. 494, 504 (1977).

[122] *See* Whalen v. Roe, 429 U.S. 589, 599-600 (1977) ("One [privacy interest] is the individual interest in avoiding disclosure of personal matters, and another is the independence in making certain kinds of important decisions.").

[123] *See* Union Pac. R. Co. v. Botsford, 141 U.S. 250, 251 (1891) ("No right is held more sacred or is more carefully guarded by the common law than the right of every individual to the possession and control of his own person, free from all restraint or interference of others unless by clear and unquestionable authority of law.").

[124] *Griswold*, 381 U.S. at 485.

couples,[125] "inter-racial" marriages,[126] abortions,[127] sodomy,[128] and haircuts.[129]

Certain aspects of informational privacy have been held to be included in this protection. The U.S. Supreme Court recognized the "individual interest in avoiding disclosure of personal matters"[130] and a legitimate expectation of privacy in the President's personal communications.[131] Also, a spousal notification requirement before an abortion was found to be likely to prevent a significant number of women from obtaining an abortion.[132] Following the U.S. Supreme Court's rulings, the majority of Circuit Courts recognized a right to informational privacy.[133]

However, the lines of the right to informational privacy remain blurry, and courts hesitate to extend the protection of informational privacy to fields that have not yet been recognized. As phrased in a dissenting opinion in Nelson v. NASA, "Is there a constitutional right to informational privacy? Thirty-two terms ago, the Supreme Court hinted that there might be and has never said another word about it. With no Supreme Court guidance except this opaque fragment, the courts of appeals have been left to develop the contours of this free-floating privacy guarantee on their own. It's a bit like building a

---

[125] *See* Eisenstadt v. Baird, 405 U.S. 438, 453 (1972).

[126] *See* Loving v. Virginia, 388 U.S. 1, 12 (1967).

[127] Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 856 (1992) (citing *Roe v. Wade*, 410 U.S. 113 (1973)).U.S.

[128] *See* Lawrence v. Texas, 539 U.S. 558, 578 (2003).

[129] *See* Kelley v. Johnson, 425 U.S. 238, 250, 153 (1976).

[130] *See* Whalen v. Roe, 429 U.S. 600 (1977); Paul v. Davis, 424 U.S. 693, 712-713 (1976) (discussing a right to informational privacy but rejecting it for the case at issue in which police had distributed leaflets with names and pictures of thieves and the words "Active Shoplifters").

[131] *See* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 427 (1977).

[132] *See* Planned Parenthood of Se. Pa., 505 U.S. at 887-88.

[133] *See* Barry v. N.Y.C., 712 F.2d 1554, 1559 (2d Cir. 1983); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577-580 (3d Cir. 1980); Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990); Plante v. Gonzalez, 575 F.2d 1119, 1132, 1134 (5th Cir. 1978); J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981) (restrictive); Bloch v. Ribar, 156 F.3d 673, 684 (6th Cir. 1998) (restrictive); Kimberlin v. United States Dep't of Justice, 788 F.2d 434, 437 (7th Cir. 1986); In re Crawford, 194 F.3d 954, 959 (9th Cir. 1999).

dinosaur from a jawbone or a skull fragment, and the result looks more like a turducken."[134]

The right to informational privacy so far appears to be limited to cases in which citizens wanted to be protected against too much government knowledge about private affairs. Government measures to 1) limit explicit disclosure by using nudges or 2) limit implicit disclosure by using compelled protection or nudges aim at preventing users from disclosing too much. Thus, they seem to be the opposite of what has been recognized so far. Neither a right not to be nudged to less explicit self-disclosure nor a right not to be prevented from implicit self-disclosure has been held to be a fundamental right. Such rights do not appear to be deeply rooted in the "Nation's history and tradition."[135]

Therefore, government acts that nudge towards less explicit self-disclosure or that restrict implicit disclosure only have to respect procedural due process of law and hence must be justified only according to the rational basis review.[136]

3. *Are the Measures Justified?*

Preventing users from excessive self-disclosure infringes upon their rights and needs to be justified.

Compelling users to refrain from explicit disclosure interferes with their First Amendment rights and faces strict scrutiny. Limiting explicit disclosure by nudges or preventing implicit disclosure can be justified according to the rational basis review. In both cases, a government interest is necessary which is compelling (First Amendment) or legitimate (Due Process Clause). Protecting users from voluntary self-disclosure which harms themselves would have to be a compelling respectively legitimate interest in order to justify the measures.

When interpreting the First Amendment, the U.S. Supreme Court states, "The First Amendment mandates that we presume that speakers, not the government, know best both what they want to say and how to say it. [...] To this end, the government, even with the purest of motives, may not substitute its judgment as to how best to

---

[134] Nelson v. NASA, 530 F.3d 865, 878 (9th Cir. 2008).

[135] Moore, 431 U.S. at 503 (characterizing fundamental rights).

[136] *See* United States v. Carolene Prods. Co., 304 U.S. 144, 152-53 (1938) (introducing the rational basis review).

speak for that of speakers and listeners; free and robust debate cannot thrive if directed by the government."[137]

Similar ideas can be found regarding the scope of the right to privacy. "As a nation [...] historically and continuously, we are irrevocably committed to the principle that the individual must be given maximum latitude in determining his own personal destiny."[138]

Both decisions are characteristic of the great importance the U.S. legal and societal system attaches to the citizens' freedom of decision. U.S. law is shaped by the liberal idea of individual freedom, irrespective of how individuals exercise their freedom and with the consequence that individuals will have to bear the costs of their shortcomings as a price they have to pay for the freedom to commit their own mistakes. The legal system is marked by freedom, moral diversity, tolerance, and government neutrality, flanked by confidence in the free market economy.

Protecting autonomous individuals against themselves would be the contrary of what the U.S. legal system aims at and thus *de lege lata* should not constitute a legitimate government interest to stand rational basis review (however, it has to be admitted that nudging could be held to be just a form of enhanced disclosure and enhanced consumer control and thus a rational economic interest).

Thus, there is no way to justify coercive measures and, at least under the current state of law, there also seems little to now way to justify nudges.

III. *A Way Out for Libertarian Paternalists?*

As an exception to the general rule that governments may not nudge users towards not disclosing personal data with the only goal of protecting their privacy, some libertarian paternalists may deny the need to justify their measures as they might not be an infringement upon the users' rights[139] in the first place.

Based on the general principle of the *homo economicus*, particularly in the United States, scholars call to deploy libertarian

---

[137] Riley v. Nat'l Fed'n of the Blind of N.C., Inc., 487 U.S. 781, 791 (1988).

[138] Rutherford v. United States, 438 F. Supp. 1287, 1300 (W.D. Okla. 1977) (deciding the question whether the use of the non admitted medicine Laetrile is protected by the right to privacy).

[139] In any case, these measures may infringe upon the data collectors' rights and thus may need justification regarding their rights. As this question does not concern the paternalistic aspects of the prevention of self-disclosure, it will not be analyzed in depth in this paper.

paternalistic measures to nudge users into limiting self-disclosure to what is in their rational interest. Such measures are not regarded to endanger the users' rights, but as an instrument to help users. Scholars structure the argument as follows:

1. *Irrational Behavior*

Neo-classical economic theory is based on the assumption that humans are rational actors who know their preferences and aim to maximize their utilities. Preferences can include non-monetary goods like happiness or the protection of privacy. As alternatives tend to be limited, rational actors choose the best available alternative. The constrained maximum is reached when marginal costs equal marginal benefits, i.e. a raise in costs would not lead to a proportionate raise in benefits.

The neo-classical view seems not to explain actual privacy behavior, though. A majority of U.S. citizens value some kind of informational privacy. In a 2012 survey in the United States, in exchange for an adequate compensation, between 81 and 93 percent of the participants were willing to reveal their gender and civil status, but only between 11 and 17 percent agreed to share their browser histories or cell phone numbers, and only 4 to 7 percent consented to share their cell phone histories or email contacts.[140] Furthermore, users seem willing to pay higher prices for privacy-enhancing products. A non-representative study in the United States showed that participants preferred more expensive products if the search engine marked them as privacy-enhancing.[141]

Still, users both explicitly and implicitly disclose vast amounts of information about themselves, though their costs in protecting informational privacy more would be relatively low, as they could for example easily disclose less or only to limited audiences or engage in privacy self-management. Thus, assuming that users value their informational privacy (as indicated by the studies), many act differently from what would be in their rational interest.

---

[140] *See* Deborah Bothun et al., *Consumer privacy: What are consumers willing to share?,* PWC.COM (May 2012), *available at* http://www.pwc.com/us/en/industry/entertainment-media/publications/consumer-intelligence-series/consumer-privacy.html.

[141] The search engine analyzed on the basis of P3P, in how far the websites' privacy policies were in accordance with the users' preferences, and accordingly marked the websites with icons, *see* Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFORMATION SYSTEMS RESEARCH 254, 254 et seq. (2011), *available at* http://www.guanotronic.com/~serge/papers/isr10.pdf.

These findings are explainable by the fact that users act predictably irrational, as behavioral economists like to put it. Individuals have a limited capacity to understand and exploit information. If a decision is too complicated, simplifying less accurate strategies are used. The complexity of the consequences self-disclosure can cause may be difficult or impossible to understand for users.[142] The plurality of data collectors and processors as well as the phenomenon of data accumulation can rarely be cognitively captured. Even if privacy policies are read, users might suffer from "information overload".[143] Professor Helen Nissenbaum describes a "transparency paradox" by stating that transparency is reached by detailed information, but too much information leads to a lack of transparency.[144] The marginal benefit of additional information might decline or even be negative. Technical innovations are difficult or impossible to foresee and consequently users may not be able to judge which future uses of their data they want to consent to.[145] Amongst others, these factors complicate the users' attempts to understand all relevant consequences and to estimate the probability of their occurrence.[146] And even if users had all relevant information and would be able to understand it, behavioral economists argue that actual behavior still differs from the behavior of a rational actor.

2. *Correcting the Shortcomings*

The described findings that users disclose data in predictably irrational ways are suggested to serve as a basis to correct these irrationalities.

Professors Richard Thaler and Cass Sunstein claim, "The presumption that individual choices should be respected is usually based on the claim that people do an excellent job of making choices,

---

[142] *See* Acquisti & Grossklags, *supra* note 55, at 364.

[143] *See* M. Ryan Calo, *supra* note 65, at 1054.

[144] *See* Helen Nissenbaum, *A Contextual Approach to Privacy Online*, DAEDALUS, THE JOURNAL OF THE AMERICAN ACADEMY OF ARTS & SCIENCES 32, 36 (2011).

[145] *See also* Mayer-Schönberger & Cukier, *supra* note 6, at 153; Solove, *supra* note 48, at 1890.

[146] *See* Acquisti & Grossklags, *supra* note 55; *see also* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1160 (2009).

or at least that they do a far better job than third parties could possibly do."[147]

Based on this assumption, liberal paternalists suggest to only respect individual choices if they are rational. If they are not, one might alter them to the decision a rational actor would have made.[148] Professor Anita L. Allen proposes "regulatory measures aimed at curbing the culture of exposure for the sake of 'forcing' people to love privacy and live privately",[149] without specifying possible constitutional justifications.

To prevent self-disclosure not in the users' rational interest, libertarian paternalists suggest using the nudges described above (see C). The surprising upshot of the libertarian paternalists' argument is that helping users to reach their rational goals even though this would mean altering their free decisions would not infringe upon their rights.

3. *Libertarian Paternalism as a Justification for Overriding Free Choice?*[150]

However, this argument does not hold up to a constitutional analysis in either Germany or the United States.

Libertarian paternalistic measures can help users to make rational choices. As long as private actors consult those measures, the users' constitutional rights are not affected as private actors are not bound

---

[147] Only in a footnote they mention that preserving autonomy could constitute a reason to reject paternalism, even if such an autonomy implies errors in decision-making. However, they limit this argument immediately: "We do not disagree with the view that autonomy has claims of its own, but we believe that it would be fanatical [...] to treat autonomy, in the form of freedom of choice, as a kind of trump not to be overridden on consequentialist grounds." Cass Sunstein & Richard Thaler, *Libertarian Paternalism is Not an Oxymoron*, *supra* note 60, at 1167 n. 22.

[148] *See* Gary Lucas, Jr., *Saving Smokers From Themselves: The Paternalistic Use of Cigarette Taxes*, 80 U. CIN. L. REV. 693, 718 (2012) ("imperfect rationality still provides a basis for paternalism"); and Robert J. Baehr, *A New Wave of Paternalistic Tobacco Regulation*, 95 IOWA L. REV., 1663, 1671-1672 (2010) (justifying warnings on cigarette packages).

[149] Allen, *Coercing Privacy*, *supra* note 1, at 753.

[150] For a broader discussion of this thought, *see* Andreas Kapsner & Barbara Sandfuchs, *Nudging as a Threat to Privacy*, 6 REV. OF PHILOSOPHY AND PSYCHOLOGY 455, 455 et seq. (2015); Cass R. Sunstein, *Nudges, Agency, and Abstraction: A Reply to Critics*, 6 REV. OF PHILOSOPHY AND PSYCHOLOGY, 511, 511 et seq. (2015).

by them. But what if the government decided to instruct libertarian paternalistic measures with the only goal of protecting competent users from making free, irrational choices regarding self-disclosure? Would this be a legitimate government interest? This paper argues that the answer to these questions is no.

Competent individuals regularly make decisions which are not in their best interest and they have a right to do so. Even if the goal of protecting users from making irrational disclosures is a laudable goal, doing so would disrespect the users' free choice. And even if nudges do not compel the users, they de facto force them to handle/reject/think about the governments' ideas of how they should live their lives. Although this aspect has not received large scholarly attention, some commentators notice that libertarian paternalistic measures begin "to circumvent traditional, liberal modes of limitation on state action and are opening up new registers of legitimate government activity", thereby "justifying the presence of the state in everyday life".[151] No matter how the governments' goals are implemented, a situation in which a government decides what is best for its citizens has to be classified as paternalistic.

The users' autonomy grants them the right to make their own decisions, even if they are non-favorable or they will be regretted later. Even a truly irrational self-disclosure remains a free self-disclosure.

As long as there is no persuading explanation on why the users' well- being should outweigh their autonomy to make free, but disadvantageous decisions, nudging users into making rational choices seems not to be justified by a legitimate governmental interest.

Notwithstanding the authors' doubts, the legal development in this area seems hard to predict. Nudges from the government regarding the users' rights need not withstand First Amendment scrutiny, but only rational basis review (see E II). Hence, the measures only need to be reasonably related to a legitimate government interest. It seems possible that courts acknowledge a government interest to protect users from making irrational choices as legitimate and thus hold that such measures do not constitute a violation of the users' rights.

Also, as infringements upon the data collectors' rights call for a higher level of justification than infringements upon the users' rights, courts may bypass investigation of violations of the users' rights and only focus on the data collectors' rights. Nudges will most likely have to face the stricter intermediate scrutiny according to the *Central*

---

[151] Jones, Pykett and Whitehead, *supra* note 57, at 483, 486.

Hudson test.[152] This will be the case if data collectors are obliged to engage in compelled speech which is not merely uncontroversial and factual, but transports a normative message.[153] All compelled speech whose primary aim is to convey the government's opinion on how individuals should act faces intermediate scrutiny.[154] In *R.J. Reynolds Tobacco Co. v. Food and Drug Admin.*, the D.C. Circuit Court ruled that graphics on cigarette packages convey not only uncontroversial and purely factual information, but aim to evoke emotions and thus change the consumers' behavior.[155] Also, mandatory privacy-enhancing defaults face intermediate scrutiny regarding the data collectors' First Amendment rights. According to the Tenth Circuit Court's ruling in U.S. West v. FCC, a FCC rule which obliged telecommunication service providers to require an opt-in before they were able collect their users' data restricted the data collectors' commercial free speech rights, as they needed to get consent before directing data-based targeting advertisement to the users. The court argued that privacy protection could serve as a substantial government interest, but the measure was not narrowly tailored, as the court could not find proof that citizens who care about their privacy would not as well protect it under a less restrictive opt-out rule.[156]

---

[152] *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 566 (1980) ("we ask whether the asserted governmental interest is substantial. […] we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest").

[153] *See* Allen Rostron, Pragmatism, Paternalism, and the Constitutional Protection of Commercial Speech, 37 VT. L. REV. 529, 571-572 (2013).

[154] *See also* Jennifer M. Keighley, Can You Handle The Truth? Compelled Commercial Speech and the First Amendment, 15 J. OF CONSTITUTIONAL L. 569 (2012).

[155] The graphics were even accompanied by the display of the phone number "1–800–QUIT–NOW" of a substance abuse counselor, *see* R.J. Reynolds Tobacco Co. v. Food and Drug Admin., 696 F.3d 1205, 1216 et seq. (D.C. Cir. 2012).

[156] *See* U.S. West, Inc. v. F.C.C., 182 F.3d 1224, 1239 (10th Cir. 1999) ("[T]he FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy. The respondents merely speculate that there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the opportunity to do so. Such speculation hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires.").

4. *Summary*

Some scholars suggest making competent adult users disclose less by either using compelled protection or nudges and thereby protect their own online privacy.

Under German law, preventing online self-disclosure infringes upon the right to informational self-determination and thus can only be justified by a legitimate government interest.

In the United States, limiting explicit disclosure by coercive measures infringes upon the First Amendment's rights of the users and needs to be justified by a compelling government interest. Using nudges to do so does not fall under the First Amendment, but triggers procedural due process protection. Likewise, preventing implicit disclosure has to meet procedural due process standards and therefore requires a legitimate government interest.

However, such paternalistic interventions lack a legitimate or compelling respective legitimate government interest and thus cannot be justified. This is true not only of coercive measures, but also of libertarian paternalistic ones.

IV. *Comparison*

Using compelled protection or nudges to prevent competent adult users from self-disclosure both in Germany and in the United States is only constitutional if the measures are justified.

The German right to informational self-determination (Art. 2 para. 1 in conjunction with Art. 1 para. 1 Basic Law) amongst others protects the users' right to self-disclosure. Government measures to prevent users from online self-disclosure with the only goal of protecting them against themselves lack a legitimate governmental interest and therefore are unconstitutional.

Under U.S. law, the First Amendment protects against compelled protection that would limit explicit disclosure. The Due Process Clause protects against nudges aimed to limit explicit disclosure as well as against compelled protection or nudges aimed at limiting implicit disclosure. Preventing self-disclosure with the only aim of protecting competent adult users from harms caused by themselves fails to pursue a compelling respectively legitimate interest and therefore is unconstitutional. To the authors' view, these findings do extend to the unconstitutionality of nudges which are solely aimed at preventing irrational behavior. Such measures will have to face a rational basis review and it is doubtful if courts will rule that they pursue a

legitimate interest. Even if courts do so, regarding the data collectors' First Amendment rights, nudges will face intermediate scrutiny.

Both the German and the U.S. society are confronted with the same harms self-disclosure can cause to individuals. Such self-disclosures can theoretically be prevented or hindered by using compelled protection or nudges. However, under both legal systems protecting competent adult individuals from themselves cannot serve as a sufficient government interest to do so.

F. CONCLUSION AND DIRECTIONS FOR FURTHER RESEARCH

It has been shown that despite the advantages of online self-disclosure, it can also cause harms to the development of the users' personalities.[157] Governments could, in theory, limit online self-disclosure by enforcing compelling privacy protection or nudging users into revealing less information about themselves.[158]

However, neither the German nor the U.S. government has the duty[159] or even the power[160] to coercively alter the privacy choices of competent adult users for the sole purpose of protecting them against harms they cause to themselves. Likewise, this paper argues that citing the irrationality of certain self-disclosures cannot serve as a justification for protecting competent adult users from these self-disclosures by liberal paternalistic means. Thus under both legal systems preventing self-disclosure with the only goal of protecting competent adult users will always violate their constitutional rights.

Nevertheless, governments are not left with tied hands. This paper suggests focusing not on preventing self-disclosure solely for the individuals' sake. A more promising route is to remember John Stuart Mill's harm principle, according to which governments may only interfere with their citizens' behavior when the welfare of others is at stake. Thus, attention should be directed towards the goal of preventing the harms self-disclosure can cause to third parties and society. Both German and U.S. courts have taken a generous approach when justifying measures that protect such interests and, as a side-

---

[157] *See* B.

[158] *See* C.

[159] *See* D.

[160] *See* E.

effect, protect competent adult individuals who voluntarily endanger themselves.[161]

The Bundesverfassungsgericht based the constitutionality of seatbelt laws on the goal of protecting third parties. In a car crash, passengers who wear seatbelts are more likely to survive and, thus, be able to help others on the scene. Also, in a crash seatbelts avoid passengers to be catapulted against other passengers in the car.[162] Similarly, the Texas Court of Appeals upheld a seatbelt law because it "serves the public safety and welfare by enhancing a driver's ability to maintain control of his vehicle, and by reducing injuries not only to himself, but also to others, all of which directly affects the state's economic welfare."[163]

A duty to wear a helmet while riding a motorbike was held to be constitutional in both jurisdictions. The Bundesverfassungsgericht argues that accidents which cause severe head injuries harm the society as an emergency rescue service and doctors have to be involved, and further medical costs arise.[164] The Texas Court of Criminal Appeals held a duty to wear helmets constitutional as it was "intended to promote the welfare and safety of the general public as well as the cyclist, and bears a reasonable relationship to highway safety generally."[165]

When upholding the prohibition of a peep show, the Bundesverfassungsgericht reasoned that such a ban aims at protecting the individuals' human dignity which is of importance not only for the individual herself, but also for society at large.[166] Similarly,

---

[161] Examples can be found in various other areas of the law: The Bundesverfassungsgericht held that regulating the consumption of drugs is constitutional as it aims at forming a society free from social harms caused by handling drugs, especially because the development of adolescents' personalities can be hindered by the consumption of narcotics. *See* BVerwGE, Mar. 9, 1994, 90, 145 (174) (Ger.). The U.S. Supreme Court held that the government can prohibit assisting suicides to promote a government interest in protecting the integrity of the medical profession and to prevent a future trend to euthanasia and further abuse. *See* Washington v. Glucksberg, 521 U.S. 702, 728 (1997).

[162] *See* BVerwG, June 6, 1987, NJW 1987, 180, 180 (Ger.).

[163] *See* Richards v. State, 743 S.W.2d 747, 748 (Tex.App-Hous. 1st Dist. 1987).

[164] *See* BVerwG, Dec. 15, 1981, NJW 1982, 1276 (Ger.). Justifying coerced protection with society's interest in saving any kind of social welfare costs however seems to be a slippery slope, as it could allow government intervention with a majority of every day life decisions.

[165] *Ex parte* Smith, 441 S.W.2d 544, 548 (Tex. Crim. App. 1969).

[166] *See* BVerfGE, Dec. 15, 1981, 64, 274 (280) (Ger.).

prostitution in the United States can be prohibited for the purpose of serving a "social interest in order and morality" (by contrast, prostitution is legal in Germany).[167]

The prohibition of smoking in restaurants in Germany was held to serve the outbalancing public interest of health protection even in tiny restaurants with no employees, in which only the owner and guests who choose to stay are affected.[168]

As these examples show, a broad interpretation of what can constitute a harm to third parties or society is licit. To justify government measures that prevent self-disclosure, it is advisable to investigate whether in the respective case there might be a government interest in such harms to others.[169]

1. *Harms to Third Parties*

Self-disclosure can indeed threaten third parties, for example if the disclosed information allows conclusions to be drawn about them. An example for explicitly disclosed harmful information would be pictures which also show third parties or status updates that involve information about them. Also, implicit disclosure can harm third parties, as big data analysis allows predictions about health, financial situation, political views, etc. not only regarding the individuals, but also regarding their family members, partners, friends, neighbors, work colleagues, etc.

Governments in fact do react to such harms, for example by imposing privacy tort laws or recognizing special professional duties of confidentiality and secrecy (and thereby coerce informational privacy).

---

[167] State v. Mueller, 617 P.2d 1351, 1359 (Hawaii 1983) (regarding the Hawaiian right to privacy).

[168] *See* BVerfGE, Jul. 30, 2008, 121, 317 (357-358) (Ger.).

[169] In an interesting recent exchange (APA Newsletter, 13 Philosophy of Law 14, 14–19 (2013), Prof. Beate Roessler suggested that Prof. Anita L. Allen, one of the most outspoken supporters of coercing privacy, should likewise concentrate on the collateral damages on third parties and society, precisely to avoid charges of paternalism. Allen responded (id. at 19–27) that she felt that there are privacy harms to individuals that should not be tied up with harms to others. Their discussion is about moral, not legal justifications of legal measures. Taking Allen's stance in the present, i.e. legal, setting, would mean to put intellectual honesty over legal pragmatism (maybe quite in accord with Allen's Kantian sympathies).

These disclosures still threaten *individualistic* privacy rights, even if the individuals harmed are different from those who disclose. Realizing that construing privacy as an essentially individualistic right diminishes its chances to prevail against competing large-scale societal values, legal scholars as well as philosophers, sociologists and other researchers have been putting ever more emphasis on privacy's value for society in general.[170]

2. *Harms to Society*

In fact, the harms on personal development and creativity that were discussed earlier (see B) can be argued to collectively amount to a threat to society that is greater than the sum of its parts. A well-functioning society depends on its members' abilities to self-govern. Only if the members can freely develop their personalities, will they be able to fully contribute to the success of society as a whole. A loss of individual informational privacy will therefore not only affect the individuals, but lead to "communities governed by apathy, impulse, or precautionary conformism".[171] The restrained creation of ideas will result in individuals not being able to contribute anything of interest to the society.[172]

Self-disclosure can harm the society both by interfering with society's progress and by constraining democracy.

a. *Harms to Society's Progress*

Free development of personalities serves as the basis for cultural, scientific and economic progress of a society.[173] Traditions have to be questioned, outdated customs to be abandoned, drawbacks to be identified, and improvements to be made. Scientific progress depends on the curiosity and courage of scientists, who are willing to take new paths. Innovations and new ideas contribute to a flourishing economy.

---

[170] *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 212-241 (1995); Solove, *supra* note 4, at 89–98; Beate Roessler & Dorota Mokrosinska, *Privacy and Social Interaction,* 39 PHILOSOPHY AND SOCIAL CRITICISM 772, 772 et seq. (2013).

[171] *See* Cohen, *supra* note 40, at 1426-1427. Similarly, Professor Neil M. Richards notes: "free minds are the foundation of a free society." Richards, *supra* note 41, at 1946.

[172] *See* Richards, s*upra* note 16, at 405; Richards, *supra* note 41, at 1948.

[173] *See also* Cohen, *supra* note 20, at 1918 et seq.

However, they can be hindered by the described obstacles that a loss of informational privacy poses to the development of the individuals' personalities.

A biased access to information can limit the users from developing new ideas that do not fit their old patterns.[174] Self-censorship regarding both the access to information and the thinking process itself can lead to societal stagnation.[175]

b. *Harms to Democracy*

A loss of informational privacy can harm the flourishing of democracy in three ways: By the effects of filter bubbles and by a self-censorship both regarding the creation and expression of ideas.

A pre-selection of online sources by filter bubbles (see B I) can create the impression, deficits would either not exist or would yet be solved by a sufficient number of other people. Thus, individuals might refrain from taking necessary actions. They might also miss problems, as people would rather read pleasant than unpleasant information.[176] Whereas a newspaper's editor will include both kinds of information, personalized search might not. As Professor Julie E. Cohen notes, in a society which is modulated by big data analysis, the individual information environment may be adjusted to the individual comfort level. To motivate citizens to take action, a "certain amount of *dis*comfort" is necessary.[177]

Furthermore, as the Bundesverfassungsgericht states, democracy depends on its members' ability to develop their personalities in a free and self-determined way.[178] A fruitful formation of the public opinion demands interested and active citizens, who reach their own conclusions and contribute to public discourse.[179] Each democracy depends on its members' autonomy, as only self-determined individuals can meaningfully contribute.

---

[174] *See* Pariser, *supra* note 18, at 23.

[175] *See* Schulhofer, *supra* note 37, at 178-179.

[176] *See also* Pariser, *supra* note 18, at 26, 81-82.

[177] *See* Cohen, *supra* note 20, at 1918.

[178] *See* BVerfGE, Dec. 15, 1983, 65, 1 (42-43) (Ger.).

[179] *See also* Regan, *supra* note 170, at 225 et seq.; Richards, *supra* note 16, at 391; Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, WIS. L. REV. 743, 761-762 (2000).

In addition, even if citizens are able to freely develop ideas, a lack of informational privacy may impede them from announcing those ideas. Participation in democratic processes is not limited to voting, but also requires citizens to express their ideas in other forms, like joining demonstrations, working for political parties or interest groups, or speaking out in social networks, blogs, etc. While doing so, some might want to reveal their identity while others might prefer not to. Any form of political speech is a very sensitive issue as citizens cannot know if it can harm them now or later in their private or business relationships. They can neither predict whether in the future they will develop different political ideas nor whether the political system as a whole may develop in an extremist direction so their past statements may harm them one day. Therefore, it is likely that users feel uncomfortable with the existence of records about their political speech and would prefer to act anonymously.

The Bundesverfassungsgericht bases the development of the right to informational self-determination on the notion that citizens who are afraid that their participation in political processes may be registered and cause risks for them, might abstain from exercising their fundamental rights to associate and demonstrate.[180] The U.S. Supreme Court acknowledges that "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance."[181] Professor Paul M. Schwartz asks: "[W]ho will speak or listen when this behavior leaves finely-grained data trails in a fashion that is difficult to understand or anticipate?".[182]

That democracy-threatening self-censorship actually happens was shown by a 2013 survey among 528 journalists in the United States. Twenty-eight percent admitted to having restricted their use of social networks due to the fear of surveillance, twelve percent considered to do so. Sixteen percent avoided talking about certain issues, eleven percent considered to do so.[183] The fact that this concerns journalists is of course especially problematic, because it feeds right into the point made at the beginning of this section - the insufficient and biased distribution of information to society at large.

---

[180] *See* BVerfGE, Dec. 15, 1983, 65, 1 (43) (Ger.).

[181] *See* Talley v. California, 362 U.S. 60, 65 (1960).

[182] *See* Schwartz, *supra* note 39, at 1651.

[183] *See* FDR Group, *supra* note 36.

c. *Other Harms to Society*

Many other harms that a loss of privacy might engender have been identified and described. The philosopher Thomas Nagel speaks out for a society in which we do not "share our inner lives, bare our souls, give voice to all our opinions – in other words, become like one huge unhappy family".[184] He goes through a number of examples in which the only way in which conversations, debates and even disagreements can be had constructively is by withholding certain information.

Prof. Daniel Solove offers that privacy acts as a mitigating factor when social norms become overbearing. Even beneficial norms, he argues, should sometimes only be "imperfectly enforced", and privacy guarantees little pockets of public un-attention to allow for this.[185]

Many researchers claim that social roles can only be successfully played if a certain degree of privacy exists. The proper relationship between a student and a teacher cannot be maintained if the teacher supplies too much personal information about him- or herself.[186]

To give one more example, and to pick up Nagel's theme with a twist: Society depends on most children getting a first sense of good citizenship from their families. However, "the family can do justice to its different functions only if it can comprehend itself as a protected private sphere."[187]

These diverse observations might well suffice to generally urge the inculcation of a more pronounced privacy ethics, and they might warrant relatively unproblematic government actions such as those discussed in the beginning of section C above.

However, it seems that limiting acts of self-disclosure, especially explicit ones, will be hard to justify with these arguments, at least as far as they are developed until now. Firstly, scholars need to get more concrete about the dangers of losses of privacy for society. The problem with many of these claims is that they are described in an unhelpfully abstract way, without examples that make the dangers palpable. For example, the only illustrative case Solove goes into in great detail regarding his point about overbearing social norms

---

[184] Thomas Nagel, *Concealment and Exposure*, 27 PHILOSOPHY AND PUBLIC AFFAIRS 1, 11 (1998).

[185] Solove, *supra* note 4, at 94.

[186] *See* Roessler & Mokrosinska, *supra* note 170, at 780.

[187] *Id.* at 775.

concerns Victorian blackmail laws. Not only is this not a very current example, it also shows, by Solove's own admission, privacy's "potential dark side" instead of its virtues.[188]

Secondly, one would need to show clearly how *self*-disclosure in particular gives rise to these dangers. It is surely true that "[i]t is hard to imagine how people could freely participate in public life without some degree of control over their reputation and private life".[189] But to turn such an observation into an argument for restricting self-disclosure, a government would have to show how unchecked self-disclosure alone might lead to such a total loss of control.

However, it may well be possible to expand these arguments sufficiently to restrict self-disclosure, especially of the implicit sort.

In that case, further research will particularly have to focus on the data collectors' rights. The German right to economic freedom (Art. 2 para. 1 Basic Law) can be relatively easily limited in order to protect the rights of others, the constitutional order, and the moral law. In the United States, by contrast, limiting access to the users' data restricts the data collectors' First Amendment rights, as the data collectors are hindered in using the data for the purpose of targeted advertisement. Hence, such restrictions are only justified when meeting the Central Hudson standard.[190] Also, nudges which compel data collectors to deliver speech which is not uncontroversial and not purely factual face intermediate scrutiny according to the *Central Hudson* standard.[191] Privacy protection serves in principle as a substantial government interest to justify such measures, but only if the government can prove significant and concrete harms.[192] Thus, the rights of the data

---

[188] Solove, *supra* note 4, at 96.

[189] *Id.* at 93.

[190] In a similar case, the U.S. Supreme Court, without further specifying its idea, recently even called for a "heightened scrutiny". *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2657 (2011) (regarding a statute that limited pharmaceutical companies' access to pharmacies' data which revealed prescription habits of doctors).

[191] *See* R.J. Reynolds Tobacco Co. v. Food and Drug Admin., 696 F.3d 1205, 1216 et seq. (D.C. Cir. 2012) (regarding graphics on cigarette packages).

[192] *See* the obiter dicta in U.S. West, Inc. v. F.C.C. 182 F.3d 1224, 1235 (10th Cir. 1999) ("[T]he government must show that the dissemination of the information desired to be kept private would inflict specific and significant harm on individuals, such as undue embarrassment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purposes of assuming another's identity. Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of

collectors in both countries will have to be taken into consideration when enacting government measures that prevent online self-disclosure. It can be expected that those rights will create a larger obstacle in the United States than in Germany.

discomfort from knowing that people can readily access information about us does not necessarily rise to the level of a substantial state interest under *Central Hudson* for it is not based on an identified harm.").