THE CASE FOR AN INFORMATION TAX: CUMULATIVE HARM IN THE COLLECTIVE MISUSE OF INFORMATION

*Ying Hu**

* Lecturer, National University of Singapore. J.S.D. Candidate, Yale Law School; LL.M., Yale Law School; LL.M., University of Cambridge; LL.B, University of Hong Kong. I would like to thank Johan Dib and Ferdinand Suba Jr. for their helpful editorial assistance.

INTRODUCTION

We are accustomed to think of privacy violations as misuses of information by one person against another person to whom that information relates. A privacy tort may be committed when someone publishes embarrassing facts about another against his will. A statutory breach of privacy may occur when a company collects sensitive information about its customers without their consent. This line of thinking is bolstered by an increasing tendency to conceptualize privacy violations as violations of context-specific informational norms.[1] According to this theory, individual incidents of privacy violation can be identified when one actor transfers information to another but fails to comply with the transmission principle applicable to that type of information or to that type of interpersonal relationship.[2]

This Article focuses on a different problem—a collection of persons uses information in a way that causes harm to an individual, despite that each individual use appears innocuous in its own context (hereafter referred to as "collective misuse of information"). "Collective" misuse of information is distinct from "individual" misuse of information not merely because, in the former case, more than one individual contributes to the imposition of harm or risk of harm. Rather, it is unique because collective misuse of information is not merely an aggregate of individual incidents of misuse. It can exist in the absence of individual misuse of information. In other words, no individual might be blameworthy for the harm or risk of harm brought about by a collective. This unique feature of collective misuse of information will become clearer as we explain

[1] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 129 (2009).

[2] *Id.* at 145.

what we mean by "cumulative harm" and "cumulative risk of harm" in Part II.

Consider the following hypothetical scenario. Sarah, a single mother living with her sister, is arrested and charged with possession of illegal drugs, which she claims to have no knowledge of. While Sarah is in custody, her arrest record is shared with public housing authority, social services, employers, and many others. Upon learning about Sarah's arrest, the public housing authority threatens to bring an eviction proceeding against her sister unless Sarah promptly moves out of public housing. Sarah's employer, on the other hand, fires her after she is repeatedly absent from work due to the arrest, subsequent court appearances, and the regular mandated report to bail officers. Having lost her job and housing accommodation, Sarah's savings depletes quickly. She is running around all day desperately searching for a cheap rental apartment and a new job. To make matters worse, since she cannot afford a nanny and sometimes has to leave her young children unattended when she is out, child protection officers consider her children at risk for neglect and are taking steps to place them in a foster home. In a few months, Sarah has lost her job, her home, her savings, and is about to lose custody of her children too, despite that she has not been convicted of any crime. She is also experiencing a tremendous amount of stress and anxiety, which has taken a toll on her health.

Unfortunately, Sarah's hypothetical story might be more real than we think in the age of big data. In her article, *Arrests as Regulation*, Eisha Jain describes in detail how arrest information is routinely shared with actors outside the criminal justice system, including immigration enforcement officers, public housing authorities, employers, social services providers, education officials, and so on.[3] Moreover, she explains how arrest information can be used to make adverse decisions about the person arrested irrespective of whether that person is eventually convicted. For example, while "an arrest report itself cannot be used to establish that a crime occurred . . . [s]ome administrative proceedings allow landlords to introduce unverified arrest reports as substantive evidence, even without testimony from the arresting officer."[4] In particular, Jain notes that public housing authorities sometimes "knowingly make decisions that affect tenants who pose no known risk to others."[5] Similar use of arrest information, according to Jain, has been found in a diverse set

---

[3] Eisha Jain, *Arrests as Regulation*, 67 STAN. L. REV. 809, 810 (2015).

[4] *Id.* at 836.

[5] *Id.*

of contexts, such as immigration enforcement,[6] employment,[7] licensing,[8] child protection services,[9] foster case,[10] and education.[11] Worse still, the person arrested may not even be aware that such inferences and adverse decisions are being made.[12]

In Sarah's hypothetical case, the public housing authority, her employer, and the child protection officers all appear to have legitimate reasons for using her arrest to inform the decision they make in regard to Sarah. While crime in public housing is a well-established problem, it can be costly for landlords to actively monitor the conduct of their tenants. By contrast, arrests serve as a cost-effective tool for public housing authorities to reduce crime and to allocate public housing, a scarce resource, to more deserving residents.[13] Sarah's employer, on the other hand, may be entitled to terminate Sarah's employment under the contract. Her employer might also have suffered financial loss due to her repeated absence from work as well as reputational loss as a result of her alleged drug offense. Finally, child protection officers have reasonable grounds to believe that someone accused of drug possession might pose a risk to her children. This suspicion is reinforced by Sarah's subsequent loss of housing and the means to provide for her children financially. While each decision to use Sarah's arrest as a proxy to make adverse inferences about her might seem reasonable, the cumulative effect of those decisions, can "far outstrip any penalty imposed by the criminal justice system."[14]

---

6 *Id.* at 829 ("Arrests play a significant role in shaping how immigration enforcement unfolds today.").

7 *Id.* at 839–40 ("A significant number of employers now also receive notifications whenever an employee is arrested and fingerprinted . . . . Some employers suspend or terminate at-will employees based on the arrest.").

8 *Id.* ("Home health care workers, security guards, and taxi drivers are among those whose employers or license providers may automatically be notified of an arrest . . . . Licensing authorities and employers have considerable discretion in deciding how to proceed after learning of an arrest.").

9 *Id.* at 841–43 ("Some local law enforcement officials have responded by taking measures to notify social services in the case of a known caretaker's arrest."). Jain highlights a case in which a person was arrested for, but not charged with, possession of marijuana, but nevertheless had her children temporarily removed from her care by child services. *Id.*; Mosi Secret, *No Cause for Marijuana Case, but Enough for Child Neglect*, N.Y. TIMES (Aug. 17, 2011), https://www.nytimes.com/2011/08/18/nyregion/parents-minor-marijuana-arrests-lead-to-child-neglect-cases.html.

10 Jain, *supra* note 3, at 843 ("[A]rrests are used to determine whether a household is a good placement for a foster child.").

11 *Id.* at 844 ("[P]olice departments may notify schools about a juvenile's contact with the criminal justice system.").

12 *Id.* at 840.

13 *Id.* at 835.

14 *Id.* at 833.

Sarah's story illustrates the crux of the problem this Article is concerned with: a collection of persons may use information about an individual in such a way that appears innocuous when each use is viewed separately, but collectively cause significant (nontrivial) harm or risk of harm to that individual.

This Article makes several contributions to the existing literature. To begin with, this Article contributes to a burgeoning literature on privacy harms. As Daniel Solove and Danielle Citron have observed in a recent article, the question of how harms involving personal data should be conceptualized has received inadequate scholarly attention.[15] Though a number of scholars have noted the harmful effects of repeated but minor privacy violations,[16] this Article represents the first serious attempt to single out collective misuse of information as a distinct type of harm, and to examine in detail the nature and cause of such harm. It goes beyond reiterating the intuitive conclusion that repeated intrusions into a person's privacy can lead to a significant amount of privacy loss in the long run. Rather, I argue that as the impact of a large number of seemingly innocuous misuses of information against an individual increases, it might reach a tipping point beyond which the harm caused to that individual is unacceptable and justifies both legal and policy responses. The difficulty lies in identifying, both at a conceptual and a practical level, when that tipping point is reached. In Part II, I propose two plausible tests for identifying collective misuse of information at a theoretical level: (a) whether one of an individual's key capabilities is undermined; and (b) whether the risk of an established harmful conduct occurring is unacceptably high.

Moreover, I provide a novel account in favor of imposing an information tax on persons who use and transmit personal information. I argue that even if a person contributing to a collective misuse of information may not be blameworthy for that misuse, he is nevertheless responsible for it in the sense that he should take steps towards minimizing such misuse. This responsibility derives from his respect for other

---

15 Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 744 (2018) (noting that "scholarship has not given the issue [of privacy harm] sufficient attention."). One exception they identify is Ryan Calo, who has taken a helpful step towards identifying privacy harms. *Id.* Calo argues that most of privacy harms can be categorized into either subjective or objective harms. M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2011). Subjective privacy harm is "the perception of unwanted observation." *Id.* By contrast, objective privacy harm is "the unanticipated or coerced use of information concerning a person against that person." *Id.* Whereas Calo's taxonomy explains why the collection and processing of information can cause harm even if no human ever sees that information, it does not provide any guidance as to when a privacy harm is sufficiently severe to warrant regulatory or judicial intervention.

16 *See, e.g.*, NISSENBAUM, *supra* note 1, at 242–43; DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 118 (Harvard Univ. Press 2008).

individuals as equals who deserve the satisfaction of their basic capabilities. It also derives from him being a member of a society whose values and ends are undermined by certain misconduct. Since the collective misuse of information is essentially a coordination problem involving a large number of persons, addressing such a problem often requires extensive knowledge about the harm caused by those persons. As such, institutional support is likely necessary to determine when and what type of intervention is required to prevent or alleviate such harm. I will argue that an information tax can help finance the establishment of those institutions. An important way to fulfil one's responsibility towards reducing collective misuse of information is to contribute to that tax.

Further, this Article forms part of an emerging body of literature highlighting the danger of cumulative harm. Recently, an increasing number of commentators have lamented the inadequate attention paid to cumulative harm, such as those from chemicals and pesticides,[17] microaggressions (i.e., subtle discriminatory behavior),[18] and accidents.[19] This Article not only identifies a similar type of problem within the privacy law context, but also offers a practical solution to address that problem.

This Article proceeds as follows: Part I highlights challenges that arise in the big data era and argues that existing responses to those challenges focus on individual misuse of information. Part II introduces the concept of collective misuse of information and explains why it is distinct from individual misuse of information. Part III argues that existing approaches are inadequate to address collective misuse of information and proposes a new information tax solution.

I. BIG DATA AND INDIVIDUAL MISUSE OF INFORMATION

A. *The Big Data Era*

We live in the big data era. Our every interaction with the outside world is increasingly being tracked: the emails we send, the photos we upload, the items we purchase, and the places we visit are increasingly recorded electronically not only by Internet giants (such as the FAANG companies),[20] but also by our employers, grocery stores, credit card companies, and the apps that we download and use every day.[21]

---

17 Sanne H. Knudsen, *Regulating Cumulative Risk*, 101 MINN. L. REV. 2313, 2314–20 (2017).

18 Christina Friedlaender, *On Microaggressions: Cumulative Harm and Individual Responsibility*, 33 HYPATIA 5, 6 (2018).

19 Lee Anne Fennell, *Accidents and Aggregates*, 59 WM. & MARY L. REV. 2371, 2373 (2018).

20 "FAANG companies" refer to Facebook, Amazon, Apple, Netflix, and Google.

21 STAFF OF S. COMM. ON COMMERCE, SCI., AND TRANSP., 113RD CONG., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MAR-

The cost of storing data has dropped exponentially in the last few decades: the price for storing one petabyte (a million gigabytes) on cloud servers dropped over 90% from 2011 to 2017.[22] As a result, more personal information has been and likely will be stored and for longer periods of time. According to a 2017 report published by IBM, we create 2.5 quintillion bytes of data every day and 90% of the world's data has been created in the last two years.[23] Just to give a sense of how big 2.5 quintillion is, one quintillion is one thousand trillions; it is estimated that 2.5 quintillion pennies can cover the Earth five times.[24]

Our data is not merely stored, but also actively transferred from person to person, company to company, and country to country. Since the Federal Trade Commission (FTC) issued its report, *Protecting Consumer Privacy in an Era of Rapid Change*, in 2012, a multi-billion industry based on the collection, analysis, and sale of personal information has gradually come out of the shadow.[25] The amount and variety of data held by data brokers is staggering. According to the FTC, the database of one broker, Acxiom, contains information "about 700 million consumers worldwide with over 3000 data segments for nearly every U.S. consumer."[26] These data brokers have numerous clients in both private and public sectors, ranging from financial services firms, insurance companies, to companies in the pharmaceutical, hospitality, and utility indus-

---

KETING PURPOSES 1–21 (2013), *available at* http://educationnewyork.com/files/rockefeller_databroker.pdf.

22 *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 18 (2015) ("In 2015, a petabyte of cloud storage will cost $100,000 per year, down 90% from $1 million in 2011."). In 2017, the cost of storing one petabyte of data reportedly ranges from $4,000 to $7,000 per month, or $48,000 to $84,000 per year. Kalev Leetaru, *Why Are We So Afraid of Petabytes?*, FORBES (Jan. 17, 2017), https://www.forbes.com/sites/kalevleetaru/2017/01/17/why-are-we-so-afraid-of-petabytes/.

23 IBM, *10 Key Marketing Trends for 2017 and Ideas for Exceeding Customer Expectations* 3, COMSENSE, http://comsense.consulting/wp-content/uploads/2017/03/10_Key_Marketing_Trends_for_2017_and_Ideas_for_Exceeding_Customer_Expectations.pdf (last visited Nov. 15, 2019).

24 Nicole Chardenet, *How Much Is 2.5 Quintillion?*, MEDIUM: YAPPN (Feb. 8, 2017), https://medium.com/@nicole.chardenet/how-much-is-2-5-quintillion-361aff053059.

25 *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE v (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf ("To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation . . . that would provide consumers with access to information about them held by a data broker."); STAFF OF S. COMM. ON COMMERCE, SCI., AND TRANSP., *supra* note 21, at 4.

26 FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 8 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. The databases of another broker, Corelogic, "include over 795 million historical property transactions, over ninety-three million mortgage applications, and property-specific data covering over ninety-nine percent of U.S. residential properties, in total exceeding 147 million records." *Id.*

tries, to educational institutions and non-profit organizations, to government entities.[27]

The value of personal information is not truly unleashed until it is processed to provide insights based on which decisions can be made. The enhanced ability to store, transfer, and analyze personal information enables people to complete tasks that they have long been performing more effectively and at a lower cost. For example, advertisers have been fighting for customer attention for many decades;[28] but platforms such as Facebook, with their vast trove of personal information, enable advertisers to target customers based on their age, ethnicity, location, major, interests, political affiliation, purchase history, personality traits, salary, car model, browsing history, and many more.[29] Imagine an advertising campaign specifically targeting Latino-American liberals aged 30 who went to an Ivy league college, earn a salary between $200,000 and $300,000 a year, live in midtown New York, have purchased Met tickets in the past 6 months, and are likely to buy a condo in the next year.[30] There has even been anecdotal evidence of how someone managed to create a three-week long secret Facebook ad campaign that targeted only one person, his roommate, which was so personal and accurate that it drove his roommate "to a state of paranoia" at a cost of merely $1.70.[31]

The ability to comb through and analyze vast amounts of data at unprecedented speed has also enabled people to connect dots that were previously hidden. In his award winning book, *Moneyball*, Michael Lewis tells a fascinating story of how Oakland A's general manager, Billy Beane, used statistics to disrupt baseball's widely accepted "scouting" theory: traditionally, scouts selected players based on their speed, quickness, arm strength, hitting ability, and mental toughness.[32] Beane and his team, on the other hand, scored players based on performance statistics called sabermetrics, which demonstrated that factors such as "on-base percentage" and "slugging percentage" were better predictors

---

27 *Id.* at 39–40.

28 *See, e.g.*, TIM WU, THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS 16–18 (Alfred A. Knopf 2016) (documenting how what he calls "attention merchants" compete for customer attention and create customer demand in the last century).

29 *See, e.g.*, Keith Collins & Larry Buchanan, *How Facebook Lets Brands and Politicians Target You*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/interactive/2018/04/11/technology/facebook-sells-ads-life-details.html.

30 *Cf. Help Your Ads Find the People Who Will Love Your Business*, FACEBOOK BUSINESS, https://en-gb.facebook.com/business/products/ads/ad-targeting (last visited Apr. 15, 2018) (showing that Facebook's tools let advertisers create targeted advertisements).

31 Brian Swichkow, *The Ultimate Retaliation: Pranking My Roommate With Targeted Facebook Ads*, GHOST INFLUENCE (Sept. 6, 2014), http://ghostinfluence.com/the-ultimate-retaliation-pranking-my-roommate-with-targeted-facebook-ads.

32 *See* MICHAEL LEWIS, MONEYBALL: THE ART OF WINNING AN UNFAIR GAME XIV (2004).

of success.[33] This new found insight enabled the Oakland A's to recruit valuable players at a significant market discount; with a budget of around $40 million, it was competitive with major league clubs such as the New York Yankees, which spent $126 million in salary in the same season.[34]

Baseball is just one of many sectors in which data analysis transforms existing practices. Take the credit scoring industry as an example. Credit scoring companies such as The Fair Isaac Corporation (FICO) previously assessed people's creditworthiness based on a limited number of criteria, including their "payment history, outstanding debt, length of credit history, pursuit of new credit, and debt-to-credit ratio."[35] Nowadays, credit scoring companies, both old and new, use a large number of data points to predict creditworthiness, many of which have little apparent connection to the latter.[36] One surprising example is how ZestFinance, a company aimed to improve the old credit scoring system, took into account variables such as whether a borrower reads terms and conditions carefully as a relevant factor determining their creditworthiness.[37]

Perhaps most importantly, data has enabled people to teach machines to perform tasks that could previously only be performed by a human. Artificial intelligence systems have been trained to "see," "hear," "write," "speak," and perform many more tasks: some are capable of identifying faces and images,[38] of recognizing and responding to our voice requests (e.g., Siri and Alexa);[39] others have been known to compose poetry,[40] prepare legal memos,[41] navigate the road,[42] and even build other artificial intelligence systems.[43]

---

33 *Id.* at 127.

34 *Id.* at XI–XII.

35 Mikella Hurley & Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 YALE J.L. & TECH. 148, 162–68 (2016).

36 *Id.* at 164–66 (describing various types of data used by credit-scoring agencies).

37 *Id.*

38 *See, e.g.*, Seema Mohapatra, *Use of Facial Recognition Technology for Medical Purposes: Balancing Privacy with Innovation*, 43 PEPP. L. REV. 1017, 1019 (2016).

39 Steven Melendez, *Google, Mozilla, and the Race to Make Voice Data for Everyone*, FAST COMPANY (Aug. 24, 2017), https://www.fastcompany.com/40449278/google-mozilla-and-the-race-to-make-voice-data-for-everyone.

40 Matt Burgess, *Google's AI Has Written Some Amazingly Mournful Poetry*, WIRED (May 16, 2016), http://www.wired.co.uk/article/google-artificial-intelligence-poetry.

41 Steve Lohr, *A.I. Is Doing Legal Work. But It Won't Replace Lawyers, Yet.*, N.Y. TIMES (Mar. 19, 2017), https://www.nytimes.com/2017/03/19/technology/lawyers-artificial-intelligence.html.

42 John Markoff, *Robot Cars Can't Count on Us in an Emergency*, N.Y. TIMES (June 7, 2017), https://www.nytimes.com/2017/06/07/technology/google-self-driving-cars-handoff-problem.html.

43 Cade Metz, *Google Sells A.I. for Building A.I. (Novices Welcome)*, N.Y. TIMES (Jan. 17, 2018), https://www.nytimes.com/2018/01/17/technology/google-sells-ai.html.

B. Individual Misuse of Information

Academics and policy makers are not oblivious to the risks and harms created by the ubiquitous collection, storage, disclosure, and analysis of personal information. However, existing data protection laws and regulations appear to focus on what I call "individual misuse of information," that is, legal or regulatory intervention is justified only where an individual's action is both (a) wrongful and (b) causes harm or serious offense to other people.[44]

Broadly speaking, a person commits a "wrong" if his violation of an established social or legal norm is indefensible.[45] Whether an action is wrongful in a specific context, however, is sometimes highly debatable. The applicable norms in that context may be unclear. Even if the relevant norms are well established, it may be questionable whether the person's violation of those norms is defensible.

An action "harms" another person if it sets back or defeats one or more of that person's interests.[46] As Joel Feinberg observes, we do not have an interest in everything we desire.[47] The object of one's interest must be sufficiently permanent and specific.[48] As a result, we do not have an interest in "passing desires" such as a craving for ice cream or an interest in "inclusive ends" such as happiness.[49] Having excluded these two types, Feinberg identifies three types of objects of interests: the first type is "immediate wants," which serve "either as means or as necessary conditions, to the advancement of more ulterior goals."[50] For example, going to bed early serves as a means to advance a more ulterior goal of good health. The second type is "welfare interests," which are the minimum necessary requirements for achieving higher and more ulterior goals. Examples of welfare interests include a "minimum level of physical and mental health, material resources, economic assets, and political liberty."[51] The third type consists of more ulterior goals that Feinberg calls "focal aims."[52] A distinguishing feature of these goals is that they are "ends in themselves" (though they also have instrumental value in furthering other objects of interests).[53] These goals, such as acquiring

---

44 *See, e.g.*, 18 U.S.C. § 2721 (2012).

45 *See* 1 JOEL FEINBERG, THE MORAL LIMITS OF THE CRIMINAL LAW: HARM TO OTHERS 112 (1987). Feinberg states that "*any* indefensible invasion of another's interest . . . is a wrong committed against him as well as harm." *Id.* However, it less clear, on his account, how to determine which invasion is indefensible.

46 *Id.* at 33.

47 *Id.* at 55.

48 *Id.*

49 *Id.* at 55–56.

50 *Id.* at 56–57.

51 *Id.*

52 *Id.* at 59.

53 *Id.* at 60.

political power or writing a book, vary from person to person.[54] As such, Feinberg depicts a network of interests that feed into each other.

Instrumental wants	→→→→ (efficacious means)	Welfare interests	→→→→ (necessary conditions)	Focal aims	→→→→ (efficacious means)	Passing wants/ instrumental wants/welfare interests/focal aims

Feinberg rightly points out that our law mainly protects vital welfare interests, such as bodily integrity and mental health, and rarely directly protects our focal aims.[55]

In contrast to "harm," Feinberg uses "offense" to refer to a miscellaneous group of "universally disliked mental states" (such as fear, anxiety, and minor pains) that are not necessarily harmful.[56] According to Feinberg, the seriousness of an offense is determined by a range of factors, including the intensity and duration of the offense, the number of people who are likely to be offended, the difficulty of avoiding the offense "without serious inconvenience to oneself," and so on.[57]

This section seeks to show how both the wrongfulness and harm/offense requirements are manifested in privacy torts, privacy legislation, and FTC enforcement actions. Part II identifies an important limit of this approach, that is, it fails to incorporate collective misuse of information, which can arise despite that no particular individual satisfies both requirements (a) and (b).

1. Privacy Torts

In their seminal article, *The Right to Privacy*, Samuel Warren and Louis Brandeis referred to pen portraiture and publication of private affairs in the press as examples of the type of conduct which a right to privacy should protect against.[58] A few decades later, William Prosser operationalized the idea of privacy as a right "to be let alone" into four privacy torts:

> (a) intrusion upon the plaintiff's seclusion ("intrusion");
> (b) public disclosure of embarrassing private facts about the plaintiff ("public disclosure of private facts");

---

54 *Id.* at 59.

55 *See id.* at 62.

56 2 JOEL FEINBERG, THE MORAL LIMITS OF THE CRIMINAL LAW: OFFENSE TO OTHERS 1 (1988).

57 *Id.* at 34–35.

58 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 213 (1890) ("[T]he right to protect one's self from pen portraiture, from a discussion by the press of one's private affairs, would be a more important and far-reaching one.").

> (c) publicity which places the plaintiff in a false light in the public eye ("false light"); and
>
> (d) appropriation of the plaintiff's name or likeness.[59]

Prosser's taxonomy of privacy torts has had a profound and long-lasting impact on American privacy law.[60] His taxonomy was adopted by the by the Second Restatement of Torts and has since been widely accepted.[61] As many have observed, "[n]early every state recognizes at least one form of [those] privacy torts."[62]

The elements of each privacy tort ensure that a defendant is not liable unless he satisfies both the wrongfulness and harm/offense requirements. A key requirement for the first three privacy torts is that the conduct complained of, be it intrusion, publicizing private facts, or putting someone in a false light, be "highly offensive to a reasonable person."[63]

This offensiveness requirement appears to play a dual role. On the one hand, it helps make sure that a guilty defendant's action gives serious offense to a large number of people by requiring that the relevant action is both "highly" offensive and offensive to "a reasonable person," a category that a predominant part of our community should fall into. If an action is highly offensive, it is likely to cause some harm to a plaintiff as well.[64] This prediction seems to bear out empirically: plaintiffs are rarely unable or unwilling to present evidence of emotional suffering in successful intrusion claims;[65] the large majority of false light cases concern "clearly disparaging" statements and therefore likely involve harm

---

59 William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

60 Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1888 (2010).

61 *Id.* at 1890.

62 *Id.* at 1917. Richards and Solove also point out various disappointing features of Prosser's taxonomy. *Id.* at 1918.

63 A person is liable for intrusion upon seclusion if he intentionally intrudes upon the seclusion of another if the intrusion is "highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977). A person who "gives publicity to a matter concerning the private life of another" is liable if the matter publicized (a) would be highly offensive to a reasonable person; and (b) is not of legitimate concern to the public. *Id.* § 652D. A person is liable for this tort if he knowingly or recklessly discloses to the public information about another person that puts the latter "in a false light" which is "highly offensive to a reasonable person." *Id.* § 652E.

64 A. P. Simester & Andrew von Hirsch, *Rethinking the Offense Principle*, 8 LEGAL THEORY 269, 288 (2002) ("This is not to say that all offensive conduct falls within the ambit of the Harm Principle. But many of the more serious forms of offense do so").

65 Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 965–66 (1989) (explaining that Post found "only a very few decisions where plaintiffs have been unable or unwilling to present any evidence of actual injury" and "as a practical matter virtually every plaintiff will allege and be able to produce some credible evidence of contingent and actual injury in the form of emotional suffering.").

to a person's reputation.[66] Both mental health and reputation are prime examples of what Feinberg calls "welfare interests," an impairment of which amounts to "harm."[67]

On the other hand, the offensiveness requirement limits the scope of those torts to cases in which a defendant has committed a wrong. As Robert Post persuasively argues, the "highly offensive" requirement seeks to characterize those social norms "whose violation would appropriately cause affront or outrage."[68] The wrongfulness of a defendant's action lies in the inexcusable violation of such social norms.[69]

The last privacy tort, which concerns misappropriation of name or likeness for one's own benefit, is quite different from the first three.[70] A person is liable for invasion of privacy if he "appropriates to his own use or benefit the name or likeness of another."[71] It is quite uncontroversial that misappropriation of a person's name or likeness harms that person, though commentators disagree as to the precise nature of the harm caused by this tort. Some argue that the harm lies in deprivation of a plaintiff's proprietary interest in the exclusive use of his name or likeness.[72] Indeed, many jurisdictions limit recovery to cases concerning commercial use of name and likeness.[73] Some claim that the relevant harm is dignitary, rather than pecuniary, in nature: the very commercialization of a person's name or likeness injures his personality, which is both "demeaning and humiliating."[74] Still others argue that this tort protects a person from interference with his control over how he presents himself to the public.[75]

---

66 Gary T. Schwartz, *Explaining and Justifying a Limited Tort of False Light Invasion of Privacy*, 41 CASE W. RES. L. REV. 885, 892 (1991).

67 1 FEINBERG, *supra* note 45, at 61–62.

68 Post, *supra* note 65, at 962–65 (explaining that Post refers to such social norms as civility rules and identifies another type of harm, "dignitary harm" or harm to a person's "social personality," which Post claims to result from every violation of a civility rule). "The most plausible interpretation of this legal structure is that the *Restatement* has empowered plaintiffs to use the tort to uphold the interests of social personality, which are *necessarily* impaired by a defendant's breach of a civility rule." *Id.*

69 *See id.* at 962–63.

70 Prosser, *supra* note 59, at 406.

71 RESTATEMENT (SECOND) OF TORTS § 652C (AM. LAW INST. 1977).

72 Prosser, *supra* note 59, at 406 ("The interest protected is not so much a mental as a proprietary one, in the exclusive use of the plaintiff's name and likeness as an aspect of his identity.").

73 DANIEL J. SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW 224 (5th ed. 2015) ("In many jurisdictions, appropriation occurs only when the use or benefit is commercial in nature – i.e., used to promote or endorse a service or product.").

74 Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 987–88 (1964).

75 SOLOVE & SCHWARTZ, *supra* note 73, at 545 ("The interest safeguarded by protections against appropriation is control of the way one presents oneself to society.").

However, this tort clearly does not always prohibit a person from using another's name or likeness for his own benefit. The "appropriation to one's own use" requirement is not satisfied, for example, when a defendant merely uses the plaintiff's name or likeness.[76] It must be shown that the defendant has sought to "tak[e] advantage of [the plaintiff's] reputation, prestige, or other value associated with him."[77] This requirement is essentially informed by, and in turn reinforces, the social norm governing use of a person's name and likeness, a violation of which would be wrongful.[78]

2. Privacy Legislation

Privacy torts, however, are only a small part of the puzzle. As Paul Schwartz has noted, the main legal response to the rise of a digital economy–typified by prevalent collection of personal data and innovative use of the same–is the Fair Information Practice Principles (FIPs).[79] FIPs are a set of internationally recognized principles concerning the collection, use, and disclosure of personal information.[80] Since the first set of principles were articulated in the 1970s, FIPs have been frequently referenced in key policy documents, such as reports issued by the Federal Trade Commission (FTC).[81] While various versions of FIPs differ from each other, they generally seek to protect an individual's privacy interests through the following means:

(a) Restrictions on the collection, use, and disclosure of personal information;
(b) Requirements that aim to ensure the quality and security of personal information;
(c) Providing individuals with certain rights to help them understand and, to some extent, control how their information is collected, used, and disclosed.[82]

Various elements of the FIPs are found in an array of legislation regulating the collection, storage, and use of personal data in various

---

76 RESTATEMENT (SECOND) OF TORTS § 652C cmt. C (AM. LAW INST. 1977) ("It is not enough that the defendant has adopted for himself a name that is the same as that of the plaintiff, so long as he does not pass himself off as the plaintiff or otherwise seek to obtain for himself the values or benefits of the plaintiff's name or identity.").

77 *Id.* at cmt. d.

78 Similarly, Daniel Solove argues that this tort "establishes what society considers appropriate for others to do in shaping a person's identity." Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 545 (2006).

79 Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 907 (2009).

80 *Id.* at 907–08.

81 *Id.*

82 *See, e.g.*, Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 MICH. L. REV. 2163, 2181 (2003).

contexts.[83] For example, the Fair Credit Reporting Act (FCRA) identifies, amongst other things, the circumstances under which a consumer reporting agency is permitted to furnish a consumer report,[84] obligated to provide access to free reports,[85] and obligated to disclose information to consumers.[86] Anyone who fails to comply with the requirements in that Act may be civilly liable for noncompliance.[87]

According to Paul Schwartz, one of the crucial differences between privacy torts and privacy legislation lie in the source of privacy rules: privacy torts "rests on the notion of shared, pre-existing norms of the private" while privacy legislations are primarily generated "through majoritarian decision-making" by a legislature.[88]

While a breach of the privacy rules established by the legislature is wrongful, it is not necessarily harmful or seriously offensive. As Justice Alito noted in the Supreme Court decision of *Spokeo v. Robins*, "a violation of one of the FCRA's procedural requirements may result in no harm."[89] He gave the example of an incorrectly reported zip code and opined that "[i]t is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm."[90] It is equally unclear whether any violation of FCRA would give serious offense to ordinary members of our community. In addition to an incorrectly reported zip code, a failure to notify a consumer that a consumer report has been procured about him for employment purposes[91] might not be highly offensive to a job applicant who expects background checks to be made in any event.

At first sight, FCRA appears to impose civil liability on persons who willfully fails to comply with any requirements under FCRA irrespective of whether a consumer suffers actual damages.[92] However, as

---

83 Schwartz, *supra* note 79, at 908 ("No single privacy statute contains all these [FIP] rules in the same fashion or form."). This approach is often referred to as a "sectoral" approach to privacy law, which contrasted with the position in many European countries in which a comprehensive piece of privacy legislation regulates the collection and use of personal information. *Id.* at 908–16. For example, the Fair Credit Reporting Act governs the use of credit reports, the Gramm-Leach-Bliley Act that of financial information and so on). *Id.* at 913, 920.

84 15 U.S.C. § 1681b(b)–(c) (2012).

85 § 1681b(b).

86 § 1681b(b)(2).

87 § 1681n.

88 Schwartz & Treanor, *supra* note 82, at 2179–81 ("Where advocates of the old privacy see privacy norms as preexisting, new privacy advocates see them as constructed largely through majoritarian decision-making.").

89 Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016).

90 *Id.*

91 § 1681b(b).

92 § 1681n ("Any person who willfully fails to comply with any requirement imposed under this title with respect to any consumer is liable to that consumer in an amount equal to the sum of (1)(A) any actual damages sustained by the consumer as a result of the failure or damages of not less than $100 and not more than $1,000 . . . .").

far as federal cases are concerned, the Supreme Court clarified in *Spokeo* that a plaintiff must nevertheless establish that the defendant's action is harmful.[93]

In *Spokeo*, the defendant, Spokeo, Inc., operates a website that publishes reports containing consumer data, such as a person's age, education, economic status, and health.[94] A brief version of such reports is freely available to users of its website, and users may obtain a more detailed version for a fee.[95] The plaintiff, Thomas Robins, learned about an allegedly inaccurate report on the Spokeo website.[96] According to Robins, the report wrongly described that "he is married with children, that he is in his 50s, that he is employed in a professional or technical field, that he has a graduate degree, and that his wealth level is higher than it is."[97] As a result, Robins sued Spokeo for willful violation of the FCRA.

The Supreme Court made clear that a plaintiff is not entitled to bring a case "whenever a statute grants [that] person a statutory right and purports to authorize that person to sue to vindicate that right."[98] To satisfy the injury in fact requirement, the Court maintains, a plaintiff must allege an injury that is both "concrete and particularized."[99] An injury is "particularized" if it "affect[s] the plaintiff in a personal and individual way."[100] "Concrete" means that the injury "must actually exist."[101] According to the Court, a concrete injury need not be "tangible" and may be satisfied by showing a "risk of real harm."[102]

Having laid down its guidance, the Supreme Court then remanded *Spokeo* to the Ninth Circuit to consider whether Robin's alleged injury was sufficiently concrete.[103] The Ninth Circuit applied a two-step test in its analysis, that is, a court must consider:

> (1) whether the statutory provisions at issue were established to protect his concrete interests (as opposed to purely procedural rights), and if so,
> (2) whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests.[104]

---

93 *Spokeo*, 136 S. Ct. at 1547.
94 *Id.* at 1546.
95 Robins v. Spokeo, Inc. (*Spokeo II*), 867 F.3d 1108, 1110 (2017).
96 *Spokeo*, 136 S. Ct. at 1546.
97 *Spokeo II*, 867 F.3d at 1117.
98 *Spokeo*, 136 S. Ct. at 1549.
99 *Id.* at 1545.
100 *Id.* at 1548.
101 *Id.*
102 *Id.* at 1549.
103 *Id.* at 1550.
104 Robins v. Spokeo, Inc. (*Spokeo II*), 867 F.3d 1108, 1113 (2017).

The Ninth Circuit answered both questions in the affirmative.[105] The first step seeks to identify a sufficiently important interest (or in the court's words, a "concrete" interest) whose violation, or threat of violation, can justify a finding of harm.[106] The court held that consumers' interest in preventing "the transmission of inaccurate information about them" satisfies this requirement for two reasons.[107] First, the ubiquitous use of consumer report in employment and other contexts renders it highly likely that inaccurate reports can cause harm to consumers.[108] Second, the type of harm caused by inaccurate consumer reports has a close relationship to another established type of harm (i.e., disclosure of false information that is harmful to one's reputation).[109]

The second step of the Ninth Circuit's test seeks to determine whether the defendant's actions "actually harm" or "actually create a 'material risk of harm'" to a concrete interest.[110] The court's analysis shows that such action must pass some threshold requirements: a "trivial or meaningless" violation of a concrete interest is insufficient.[111] Despite that the inaccuracy was "seemingly flattering" and that it is not always easy to determine whether an inaccuracy harms or helps an individual, the Ninth Circuit nevertheless found that the inaccuracy was not trivial and posed "a sincere risk of harm to the real-world interests that Congress chose to protect with FCRA."[112]

In light of the above, the *Spokeo* line of cases reaffirms the need to prove that a defendant's action is both wrongful (i.e., violation of a legal rule) and harmful (i.e., posing a nontrivial risk to impair a concrete interest).

3. FTC Enforcement Cases

As Daniel Solove and Woodrow Hartzog have observed, the FTC has been enforcing privacy policies mainly through its authority under section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[113] While almost all of FTC's enforcement actions result in settlements, Solove and Hart-

105 *Id.* at 1113, 1117.
106 *Id.* at 1114.
107 *Id.* at 1113.
108 *Id.* at 1114.
109 *Id.* at 1115.
110 *Id.*
111 *Id.* at 1116.
112 *Id.* at 1117.
113 15 U.S.C. § 45 (2012). The FTC has also been given rulemaking and/or enforcement authority under various privacy legislation, including Children's Online Privacy Protection Act, Gramm-Leach-Bliley Act, and so on. For a summary of the FTC's enforcement authority, see Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 602–04 (2014).

zog claim that its privacy jurisprudence has become an "influential regulating force on information privacy" and is "functionally equivalent to a body of common law."[114]

A cursory examination of the two grounds of enforcement—"deceptive" and "unfair" acts and practices—suggest that the FTC targets actions that are not only wrongful but also harmful. According to various FTC statements, an "unfair" or "deceptive" act or practice is a "representation, omission, or practice that is likely to mislead the consumer acting reasonably in the circumstances, *to the consumer's detriment*" or a practice that "*causes or is likely to cause substantial injury to consumers* which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[115]

II. COLLECTIVE MISUSE OF INFORMATION

Having established that existing privacy law mainly focuses on individual conduct that is both wrongful and harmful, this part seeks to show how the current approach fails to take into account harms caused by a collection of individuals. It will explain what collective misuse of information is and in what sense a person is responsible for contributing to a collective misuse.

A. John's Story

Let us consider another hypothetical story. John starts to experience onset of bipolar disorder in his early twenties. Like many bipolar patients, he goes on a shopping spree when he suffers from a significant mood swing.[116] Shopping websites, while unaware of his illness, notice that John is 300% more likely to purchase products during certain times, and especially after he has been to a pub or goes home late. They therefore start to collect publicly available information about John's locations and follow him on social media. Whenever John has been to a pub or has been active online late at night, these websites will serve more advertisements to him about luxury products. Unable to resist the temptation, John finds himself spending most of his money on luxury items that he does not need.

As a result, John is forced to move to a smaller apartment in a poorer neighborhood. To his dismay, his bank lowers his credit limit after the move and charges him a higher interest rate when he subsequently applies for a car loan. At the same time and unknown to John, he is also paying a higher price when he purchases goods from certain websites.

---

114 Solove & Hartzog, *supra* note 113, at 585–86.

115 *Id*. at 599 (emphasis added).

116 Jane Collingwood, *Spending Sprees in Bipolar Disorder*, PSYCHCENTRAL (Oct. 8, 2018), https://psychcentral.com/lib/spending-sprees-in-bipolar-disorder/.

John has been searching for more information about bipolar disorder online and sharing his symptoms in public discussion forums. Since then, he starts to receive more advertisement both online and offline about products that claim to "cure" bipolar disorder. Since he has not shared his health problems with his colleagues, John finds it highly embarrassing when one of his colleagues sees a Google ad about bipolar disorder on his computer screen. He is also irritated by the dozens of emails and pamphlets about bipolar disorder that he receives on a regular basis.

His mood swings have unfortunately made it harder and harder for him to get along with his coworkers and his boss, who fires John after a few unhappy incidents. While looking for a new job, John is often required to complete aptitude tests, which, to his surprise, disqualify him from even many minimum wage jobs. In one of the interviews that he manages to attend, his potential employer casually mentions some concerns about him being irresponsible. It is not until much later that John becomes aware of an online report about him that highlights his propensity to engage in impulse shopping and concludes that he might suffer from some mental illness. In addition, John receives a much higher quote for medical insurance than most men of his age, which he cannot afford, and for car insurance, which he has no choice but to pay for since public transportation is almost nonexistent in the poorer neighborhood where he lives.

John does not quite understand how he has become almost unemployable, uninsurable, and poor. His frustration causes him to resort to heavy drinking more regularly, which triggers more mood swings. Jumping from one temporary job to another, he has little money to spare on treating his mental illness and little time or effort to investigate how he ended up where he is.

Similar to Sarah's story in the beginning of this Article, John's story is more plausible than we think in the age of big data. There is increasing evidence that banks, employers, insurance companies, and various goods and other services providers use ever more granular information to approach their customers in order to maximize profit.[117] A growing number of companies place targeted advertisement based on a combination of factors such as location, purchasing history, and time.[118] For instance, a spirits company has reportedly targeted customers aged 21 to 34 "while they were in neighborhoods with lots of bars and restaurants;" a hotel booking website, on the other hand, targets travelers who, due to flight

117 *See, e.g.*, Robert D. Hof, *Marketing in the Moments, to Reach Customers Online*, N.Y. TIMES (Jan. 17, 2016), https://www.nytimes.com/2016/01/18/business/media/marketing-in-the-moments-to-reach-customers-online.html.

118 *See id.*

cancellation, are stranded at airports.[119] Some companies charge different prices for the same product depending on where their potential customers are located. For example, Staples.com has reportedly displayed different prices to different customers after estimating their locations, taking into consideration factors such as the "distance from a rival brick-and-mortar store."[120] Another journalist discovered that The Princeton Review charges nearly double price for SAT prep tests in regions whose residents are predominantly Asian.[121] While these examples of price discrimination might be incidental, other companies seem to exploit people's vulnerabilities intentionally: one research company has allegedly advised brands to market beauty products on Monday mornings, when women tend to feel less attractive.[122]

As noted in Part I.A., credit card and credit scoring companies have already embraced an "all data is credit data" approach to lending. What a person purchases and where he purchases it can affect his credit. According to one intriguing report, American Express lowered cardholders' credit limits significantly because they shopped at the same establishments where "[o]ther customers who have used their card . . . have a poor repayment history with American Express."[123] Spending half of one's income in a cheap city "could indicate profligacy" to a non-conventional credit scoring company like ZestFinance.[124] Therefore, it would not be surprising that John's shopping sprees, his inability to hold onto a job, and even the poor neighborhood that he lives in can be treated as signs of a high risk borrower.

In a similar vein, insurance companies have made use of the increased availability of data and predictive analytics in deciding whether to insure someone and at what cost.[125] For instance, automobile insurers have sought to persuade policyholders to install in their cars devices that track their driving practices, which are in turn used to determine their

---

119 *Id.*

120 Jennifer Valentino-DeVries et al., *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J. (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323772045781893918138815 34.

121 Emil Guillermo, *Do Asians Pay More for SAT Test Prep? Report Finds 'Tiger Mom Tax*,' NBC NEWS (Sept. 2, 2015), https://www.nbcnews.com/news/asian-america/report-princeton-review-s-overcharging-asians-called-tiger-mom-tax-n420401.

122 Rebecca J. Rosen, *Is This the Grossest Advertising Strategy of All Time?*, ATLANTIC (Oct. 3, 2013), https://www.theatlantic.com/technology/archive/2013/10/is-this-the-grossest-advertising-strategy-of-all-time/280242/.

123 Ron Lieber, *American Express Kept a (Very) Watchful Eye on Charges*, N.Y. TIMES (Jan. 30, 2009), https://www.nytimes.com/2009/01/31/your-money/credit-and-debit-cards/31money.html.

124 *See* Quentin Hardy, *Big Data for the Poor*, N.Y. TIMES: BITS (July 5, 2012), https://bits.blogs.nytimes.com/2012/07/05/big-data-for-the-poor.

125 Max N. Helveston, *Consumer Protection in the Age of Big Data*, 93 WASH. U. L. REV. 859, 878–80 (2016).

premium rates.[126] Casualty insurers have taken into account policyholders' social media profiles in their coverage decisions.[127] One of the more extreme examples involves Mrs. Shelton from Louisiana, who reportedly could not get health insurance from multiple insurance companies because she was previously prescribed an antidepressant and a blood pressure medication.[128] In light of existing practices, it is not inconceivable that insurance companies might seek to charge John in our hypothetical example an exorbitant premium for their services or refuse to insure him outright.

Last but not least, employers increasingly use aptitude tests to screen job applicants. As Frank Pasquale has noted, 16% of major retail hiring used "black box personality tests" in 2009.[129] These tests often require applicants to choose multiple choice answers to statements that are seemingly unrelated to their ability to perform the relevant tasks, such as "In your free time, you go out more than stay home."[130] These tests might be used, intentionally or unintentionally, to screen out people with mental illness.[131] For example, Kyle Behm, a university student who suffered from bipolar disorder, found himself repeatedly rejected even from minimum wage jobs.[132] In an attempt to understand what went wrong, he was informed by one of the companies that he was "redlighted" by the personality test that he took when applying for that job.[133]

B. Absence of Individual Misuse of Information

John's story shows that a great number of persons, legal or natural, have used John's personal information to his detriment. Viewed individually, however, the action of each person might appear quite innocuous in its own context. The reason is twofold. First, the amount of loss that many of the individuals inflicted on John is so small that it alone does not cause a "harm" to John's interests according to Feinberg's definition of harm.[134] Second, it is arguable that none of them have violated any established social or legal norm and therefore have not "wronged" John.

---

126 *Id.* at 879.

127 *Id.* at 880.

128 FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 26–27 (Harvard Univ. Press 2015).

129 *Id.* at 37.

130 *Id.* at 36.

131 *See, e.g.*, Cathy O'Neil, *How Algorithms Rule Our Working Lives*, GUARDIAN (Sept. 1, 2016), http://www.theguardian.com/science/2016/sep/01/how-algorithms-rule-our-working-lives.

132 *Id.*

133 *Id.*

134 *See* 1 FEINBERG, *supra* note 45.

1. Small Harm

A shopping website that has served location-based or time-based advertisements to John is likely to argue that each advertisement has at best occupied a few seconds of John's time. To the extent that John proceeds to buy the products advertised, the advertisements have benefited rather than harmed him since they facilitate the satisfaction of genuine preferences formed by John. A company sending John bipolar disorder advertisements might also argue that the cost those advertisements have inflicted on John is quite minimal. All he has to do is delete the relevant email or throw away the pamphlets sent to his address. While it is unfortunate that John feels embarrassed when someone else sees the advertisement, his temporary discomfort is not sufficiently serious to be considered a harm to his interests.

A shopping website displaying higher prices to John based on his location might claim to have caused him no harm either. If John is unhappy with the price, the website may argue, he is free to ignore its products and search for cheaper alternatives elsewhere, which are often only a few clicks away. Similarly, John's bank, medical insurance, and car insurance company might each point out that it purports to charge John higher interest rates or premiums based on his credit score and risk profile. In any event, John is free to approach other banks or insurance companies that offer better terms.

An employer that refuses to offer John a job might accept that John has incurred some cost in completing the relevant aptitude tests and interviews. Nevertheless, it is likely to maintain that such cost is too insignificant in itself to be considered harmful to him.

2. Absence of Wrongdoing

Has anyone committed any wrong against John? If we tweak the facts a little, one could have. For example, John could have sued his employer for wrongful termination if he were fired because of his mental illness. But I have constructed the hypothetical to ensure that none of the persons who contribute to John's loss have clearly breached any social or legal norm.

In the absence of knowledge or intention to exploit John's mental illness, a shopping website can hardly be faulted for sending John advertisements at times and places that they believe to be most effective. Likewise, if a pharmaceutical company obtains John's contact information in a public forum, using that information to promote its products seems fair play.

At first blush, many people may frown upon the practice of displaying different prices for the same product based on customer location. But a company might have legitimate business reasons for doing so. For ex-

ample, it might be more expensive to ship products to certain places or the demand for certain products might be higher in others. After all, companies do routinely charge different prices for the same product in different countries. Moreover, consumers have the opportunity to shop around before making a final purchase.

John's bank is likely to argue that John's past purchase patterns, his mental illness, and even the places he frequents suggest that the likelihood of him making full repayment on time is lower. It is only fair that the bank charges a higher interest rate to compensate for the higher risk it is taking in lending John money. Similar reasoning applies to his car insurance company. Since people suffering from bipolar disorder are more accident-prone, there is a higher chance that John might get into an accident, which justifies the higher premium.[135]

Finally, a prospective employer may not intentionally seek to disqualify applicants with bipolar disorder, but rather uses a scoring algorithm that unintentionally disfavors people with bipolar disorder. For example, the algorithm might conclude that John's frequent visits to bars, failure to make credit card payments in full, and potential sleeping problems are indications that he is less likely to perform well at work. On the face of it, these factors have nothing to do with bipolar disorder, but nevertheless they are likely to have a disproportionate impact on people with bipolar disorder.

C. Cumulative Harm

As noted in Part I, harm is generally understood as a setback of one's interest.[136] Not all harms are sufficiently serious to be considered worthy of legal redress.[137] Nevertheless, a single harm, which of itself is deemed trivial, may be combined with other equally insignificant harms to form a sufficiently serious one. A more familiar example of this phenomenon is "death by a thousand paper cuts."

1. John's Story Revisited

As explained in the previous section, each person who uses John's information to make decisions about him might only inflict a small amount of loss on him. Nevertheless, the cumulative effect of such losses can be quite substantial. As indicated in the hypothetical case, even if

---

135 Felix M. Segmiller et al., *Driving Ability According to German Guidelines in Stabilized Bipolar I and II Outpatients Receiving Lithium or Lamotrigine*, 53 J. CLINICAL PHARMACOLOGY 459, 459 (2013).

136 1 FEINBERG, *supra* note 45, at 112; Solove & Citron, *supra* note 15, at 747 ("Generally speaking, harm is understood as the impairment, or setback, of a person, entity, or society's interests.").

137 Solove & Citron, *supra* note 15, at 747 (noting a subset of "legally cognizable harm[s].").

only a small number of shopping websites manage to persuade John to buy products that he does not need or at prices that is higher than what he could obtain elsewhere, it might be sufficient to deplete most of his savings, forcing him to move to a poorer neighborhood. In addition, his occasional shopping sprees might have more far reaching consequences: for example, it can be taken into account in calculating his credit score, thereby causing him to be charged a higher interest rate than he otherwise would have been. They might even affect his job opportunities if such purchase patterns are found to correlate with irresponsible or unpredictive behavior.

Moreover, moving to a poorer neighborhood can lower his credit score, thereby reducing his ability to obtain future loans at affordable interest rate. It might even affect his job prospects: one company has found a correlation between travel distance between home and work and job performance.[138]

Further, as many researchers have pointed out, each person has limited willpower.[139] Having to constantly resist the temptation of impulse shopping can be a serious drain on John's willpower reserve, leaving him less mental strength to deal with other stressful situations (e.g., obtain a large loan or overcome difficulties at work). As a result, he might be more easily taken advantage of by other vendors.

Finally, John's inability to obtain a stable or rewarding job can feed into his existing mental and financial problems, causing more frequent episodes of mood swings, substance abuse, or impulsive shopping, thereby leading to a downward spiral.

As a result, a series of seemingly innocuous events have the potential to cause John to suffer setbacks to a number of important interests, such as access to affordable accommodation, to stable employment, to reasonable opportunity to explore other life goals, and so on.

2. Legally Recognized Cumulative Harm

In other contexts, the cumulative nature of harm has received judicial recognition at the highest level. Drawing on established criminal procedure doctrines, Kerry Abrams and Brandon Garrett demonstrate how courts, in various cases, take a holistic view of the cumulative effect of minor violations which "add up to a harm of constitutional magnitude."[140] For example, in *Taylor v. Kentucky*, the Supreme Court appears

---

138 Don Peck, *They're Watching You at Work*, ATLANTIC (Dec. 2013), https://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/.

139 *See* ROY F. BAUMEISTER & JOHN TIERNEY, WILLPOWER 1–2 (The Penguin Press, Reprint ed. 2012).

140 Kerry Abrams & Brandon L. Garrett, *Cumulative Constitutional Rights*, 97 B.U. L. REV. 1309, 1313 (2017) ("The first type, aggregate harm cases, occur when multiple discrete

to suggest that the court's "skeletal instructions" and the prosecutor's actions, while not necessarily improper when considered separately, together "created a genuine danger that the jury would convict petitioner [based on] extraneous considerations."[141] Another example cited by Abrams and Garrett involves the doctrine of ineffective assistance of counsel.[142] According to *Strickland v. Washington*, courts, when determining whether a counsel's performance is defective, should not simply look at separate incidents of errors, but should consider the "totality of the evidence."[143]

Outside the courtroom, a more familiar example of cumulative harm is pollution. If only a few persons emit a pollutant, such as carbon dioxide, it is probably not harmful to our environment, which is capable of absorbing a certain amount of chemicals.[144] If, however, a large number of persons emit the same pollutant, even a small amount, the total amount of pollutant may exceed the maximum safe level and lead to an environmental crisis.[145] If left unregulated, each person has incentive to emit as much pollutant as he can, since he enjoys the full benefit of emitting pollutant, but bears only a fraction of the cost.

3. Formalizing Collective Misuse of Information

One way to formalize John's problem and other examples of cumulative harm is through the lens of "tragedy of the commons," a paradigm for situations in which people overuse a common-pool resource "in pursuing their own interests that collectively they might be better off if they could be restrained, but no one gains individually by self-restraint."[146] A typical example of the commons problem is overgrazing. In his seminal

---

acts, taken together, add up to a harm of constitutional magnitude, even if each individual act, taken alone, would not, or would not be sufficient to obtain a constitutional remedy.").

141 Taylor v. Kentucky, 436 U.S. 478, 487 (1978) ("The prosecutor's description of those events was not necessarily improper, but the combination of the skeletal instructions, the possible harmful inferences from the references to the indictment, and the repeated suggestions that petitioner's status as a defendant tended to establish his guilt created a genuine danger that the jury would convict petitioner on the basis of those extraneous considerations, rather than on the evidence introduced at trial."); *id.* at 487 n.15 ("Because of our conclusion that the cumulative effect of the potentially damaging circumstances of this case violated the due process guarantee of fundamental fairness in the absence of an instruction as to the presumption of innocence, we do not reach petitioner's further claim that the refusal to instruct that an indictment is not evidence independently constituted reversible error."). For a similar interpretation of *Taylor*, see Abrams & Garrett, *supra* note 140, at 1317.

142 Abrams & Garrett, *supra* note 140, at 1315.

143 Strickland v. Washington, 466 U.S. 668, 695 (1984). For more details, see Abrams & Garrett, *supra* note 140, at 1318–19.

144 *See generally* Brad Plumer & Nadja Popovich, *Why Half a Degree of Global Warming Is a Big Deal*, N.Y. TIMES (Oct. 7, 2018), https://www.nytimes.com/interactive/2018/10/07/climate/ipcc-report-half-degree.html.

145 *Id.*

146 THOMAS C. SCHELLING, MICROMOTIVES AND MACROBEHAVIOR 111 (2006).

paper, *The Tragedy of the Commons*, Garret Hardin invites readers to imagine a group of herders having access to a common-pool resource, a pasture.[147] Each herder enjoys direct benefit of adding additional cattle to the pasture, but only suffers a portion of the loss from deterioration of the pasture due to overgrazing.[148] As such, a herder is motivated to increase his cattle even though he would be better off if all herders collectively limit the number of cattle on the pasture.[149] This story has often been used to illustrate the paradox that "individually rational strategies lead to collectively irrational outcomes."[150] It is also worth noting that the commons problem does not arise until a group of herders have added more sheep than a pasture can sustain. Before that tipping point is reached, there is no tragedy.

Analyzing cumulative harm as a commons problem raises several questions: What is the relevant common pool resource for the purpose of our analysis? When does a "tragedy" occur? Why does the "tragedy" occur? I now address these questions in turn.

a. The Individual as a Common Resource System

According to Elinor Ostrom, resource systems are best thought of as "stock variables that are capable, under favorable conditions, of producing a maximum quantity of a flow variable without harming the stock or the resource system itself."[151] A resource system is "common" in the sense that it is sufficiently large as to render it costly to exclude people from using it.[152] In a subsequent work, Ostrom identifies three features of a common pool resource: it is (a) available to more than one person; (b) difficult to be excluded from users; and (c) subject to "degradation as a result of overuse."[153]

One of the early scholars to draw on the idea of common pool resource in the context of information privacy law is Priscilla Regan.[154] She argues that "[t]he flow of information about personal movements

147 Garrett Hardin, *The Tragedy of the Commons*, 162 SCI. 1243, 1243–48 (1968).
148 *Id.*
149 *Id.*
150 ELINOR OSTROM, GOVERNING THE COMMONS 5 (Cambridge Univ. Press 1990).
151 *Id.* at 30.
152 *Id.*
153 COMM. ON THE HUMAN DIMENSIONS OF GLOB. CHANGE, NAT'L RES. COUNCIL, THE DRAMA OF THE COMMONS (Elinor Ostrom et al. eds., 2002).
154 *See* Priscilla M. Regan, *Privacy as a Common Good in the Digital World*, 5 INFO. COMM. SOC'Y. 382, 392 (2002). Other scholars have also drawn on the tragedy of commons idea. *See, e.g.*, A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713, 1731 (2015) ("To the extent that the diminishment of privacy in public spaces or online is caused by users taking pictures of each other and then posting them online, we do have a closer analogy to the classic tragedy of the commons: everyone is drawing from the common stock of public privacy.").

and transactions in both the physical world and the digital world" can be viewed as a common resource system.[155] Not only is personal information available for appropriation by multiple persons, Regan asserts, it is also difficult to exclude appropriators from accessing that information since most websites permit the tracking of people's activities online.[156] Moreover, she appears to claim that personal information can be "overused" in three senses. First, people might "pollute[ ]" the system with "inaccurate, irrelevant, and out-of-date information."[157] Second, people might provide less personal information to replenish the system as they distrust or resent certain secondary usage of their information.[158] Third, the value of personal information to each appropriator might decrease as more people possess the same information.[159]

Building upon Regan's analysis of the commons problem, this Article makes two additional observations in respect of collective use of personal information. Firstly, the commons problem can exist at both a collective and individual level, in other words, both an individual's or a group of individuals' personal information can be overused.[160] It is unclear whether Regan envisages each individual's personal information as a separate common pool resource or a giant common pool resource consisting of everybody's personal information. This Article prefers to analyze the commons problem at the individual level for two reasons: one theoretical, one practical. The theoretical reason is based on an objection commonly raised against aggregative theories such as utilitarianism. If the ultimate goal is to maximize the aggregate value of the personal information of a group, it is theoretically permissible to sacrifice one individual for the greater good. For example, nothing prevents us from stripping a person of all his privacy to enhance the value of the group's personal information (e.g., consider Truman Burbank in the movie The Truman Show, who, unknown to himself, lived in a simulated world for a television show since his birth, exposing every detail of his life for the entertainment of millions of viewers).[161] The practical reason lies in the fact that it is likely more difficult to assess whether the personal information of a group of individuals has been overused than whether that of an individual has.

Secondly, as Regan also recognizes, the idea of treating a person's information as a common pool resource is odd in one respect: an important feature of a common pool resource is that the resource (i.e., the

155 Regan, *supra* note 154.
156 *Id.* at 393.
157 *Id.* at 400.
158 *Id.* at 393.
159 *Id.* at 400.
160 *See id.* at 400.
161 THE TRUMAN SHOW (Paramount Home Entertainment, Special ed. 2005).

stock) is capable of producing a limited number of extractable units (i.e., flow variables); the stock is harmed (or overused) if we extract more flow variables than the limited number.[162] However, if the relevant flow variable is personal information, which is generally considered a non-rivalrous good, then presumably the stock can never be overused.[163]

This apparent objection against treating personal information as a common pool resource can be met if we stop treating actual copies of personal information as flow variables. Regan's analysis of how personal information can be overused implicitly adopts this strategy.[164] Her argument essentially treats the value of personal information, as opposed to the sheer volume of personal information, as the flow variable in question: the total value of a pool of personal information presumably decreases when it becomes less accurate or out-of-date; additionally, the value of that information to each recipient decreases as more recipients have access to it.[165] The success of this strategy depends on the accuracy of the premise of her argument, which is, the value of personal information is a rivalrous good, which can be decreased by overconsumption.[166] Evaluating the merit of this premise in turn raises a vexing question: how do we assess the value of personal information?

While there has not been a definitive answer to this question, we can envisage two general approaches to addressing it. First, we can ask an individual (A) to assess the value of his information. Second, we can assess the value of A's information from the perspective of an information recipient (B). Since we normally evaluate a common pool resource from an external perspective, let us take the same approach here. Broadly speaking, a recipient may derive value from A's information from three sources:

(1) an increase in the transfer of value from A to B;
(2) a decrease in the transfer of value from B to A; and
(3) an increase in B's value (but not at the expense of A).

Examples of (1) include identify theft and certain direct marketing campaigns. In both cases, B receives a surplus value at the expense of A. The difference lies in the amount of value A receives in return: from negative value in the case of identity theft to the equivalent of the value received

---

162 Regan, *supra* note 154, at 393.

163 *See id.* at 392–93 ("The resource system of personal information can be used jointly and particular units can be used jointly. For example, if one organization records the fact that an individual made a certain transaction or action another organization may similarly be able to record that fact. This would then distinguish information from other, especially tangible, resource units.").

164 *See id.* at 392–93, 400.

165 *See id.*

166 *Id.*

by B (in the form of goods). Examples of (2) include fraud detection and other measures to screen out undesirable customers (e.g., an insurance company might refuse to insure A if his personal information suggests that he is a high risk candidate). Examples of (3) include cases in which an exchange of goods/services that benefit both A and B or other win-win situations (e.g., where A's personal information is used to prevent the spread of communicable diseases).[167] These categories are not mutually exclusive.

More often than not, an information recipient uses an individual's information in a way that both increases that individual's benefit and imposes a cost on him. For convenience, let us call this individual John again. For example, Facebook provides a new way for John to stay connected with his friends and family, but it also exposes him to malware attacks, phishing scams, targeted advertising, and fake news.[168] This Article does not resolve the important and longstanding question of whether any specific use of personal information is worthwhile from a cost-benefit perspective. Rather, it makes a more basic point—that from the perspective of an information recipient, the value of John's personal information is a function of the total amount of value that John is capable of conferring upon that type of recipient. Take the following pool of information as an example: John likes blue jeans; on average, he spends $500 on jeans and $5,000 on clothes per year. The value of that information to all jeans sellers is likely capped at $500 per year. Even assuming that those jeans sellers manage to miraculously increase John's preference for jeans such that he spends all his clothing budget on jeans, the value of that information is nevertheless likely capped at $5,000. By analogy, the value of all information relating to John is capped by the total amount of value that John is capable of conferring on other people. If all sellers collectively spend more than $5,000 in persuading John to buy jeans, they have collectively incurred more costs than they can receive, which is wasteful from their collective perspective.

Viewed in this light, instead of treating the value of John's information as a common pool resource, it appears more apt to treat John himself as the common pool resource. He appears to satisfy all three features of a common pool resource proposed by Ostrom.[169] John is accessible to a range of persons, natural or legal, around him. He is also capable of

---

167 *See, e.g.*, MICROSOFT, *The Future Computed* 43 (2018), https://news.microsoft.com/cloudforgood/_media/downloads/the-future-computed-english.pdf (explaining the role of A.I. in preventing disease outbreaks).

168 Aatif Sulleyman, *Hackers Infect Facebook Messenger Users with Malware that Secretly Mines Bitcoin Alternative Monero*, INDEPENDENT (Dec. 22, 2017), https://www.independent.co.uk/life-style/gadgets-and-tech/news/digmine-facebook-messenger-cryptocurrency-mining-malware-monero-bitcoin-a8125021.html.

169 NAT'L RES. COUNCIL, *supra* note 153.

producing various types of "flow variables" to people who interact with him (for example, John's employer benefits from his work product, his jeans seller from his money, and his friends from his companionship).

4. Identifying Collective Harm

A crucial question is whether recipients of John's personal information can collectively extract so much value from his information that John, as a common pool resource, is "overused?" It is relatively easier to determine whether a traditional common pool resource (such as a meadow, a fishing pond, or a bridge) is overused. In the thought experiment proposed by Hardin, a meadow is overused if the maximum number of animals that can graze on the meadow is exceeded.[170] A basin is overused if withdrawals from the basin exceed its safe yield.[171] However, it is much more difficult to determine when an individual (John) is "overused."

In the following sections, I propose two possible scenarios in which John may be legitimately treated as having been "overused."

a. First Overuse Analysis: Harm to a Fundamental Interest

One possible approach to overuse is to ascertain the overall amount of value that John is capable of providing to other people at a sustainable rate. Any significant decline in that amount over an extended period may serve as an indication that he has been "overused." However, a number of problems exist with this approach. First, the benefits that John provides to other people invariably differ in kind (ranging from monetary to emotional benefit) and may not be commensurable. As such, it may not be appropriate to aggregate such benefits by reference to a single metric.[172] Second, even if we assume commensurability, choosing a benchmark and measuring various types of benefit against that benchmark can be a daunting task. One might, for example, try to use market value as a metric. However, market value might not accurately reflect the true value of the benefit John provides to others. Moreover, though the market value of John's labor is readily ascertainable by reference to his salary, it calls for much speculation when we try to gauge the market value of other activities (such as providing care and companionship) for which a market does not exist.

An alternative approach is to consider John "overused" if his well-being falls below a certain threshold. In this regard, the capability theory pioneered by Amartya Sen provides useful guidance for evaluating a person's wellbeing. Sen claims that one's wellbeing should be assessed by

---

170 Hardin, *supra* note 147, at 1244–45.

171 OSTROM, *supra* note 150, at 112.

172 AMARTYA SEN, INEQUALITY REEXAMINED 51–55 (Oxford Univ. Press 2009) (1992).

reference to capabilities and functionings.[173] Functionings consist of "being and doings," which can vary from "being adequately nourished" to more complex achievements such as "having self-respect."[174] Capability, by contrast, is "a reflection of the freedom to achieve valuable functionings."[175] Following this approach, John may be considered "overused" if any of his capabilities or functionings falls below a minimum threshold that is deemed necessary for him.[176]

This Article prefers the second approach. In spite of inevitable ambiguities associated with this approach, it avoids committing to the implausible position that most of the goods and activities valued by our society are commensurable. Moreover, this approach can still shed valuable light on collective misuse of information even if we fail to identify every essential capability. By contrast, if we adopt the first approach, our analysis would hinge on identifying the correct metric for valuing human activities. Further, much progress has been made in the last few decades, particularly by Amartya Sen and Martha Nussbaum, in identifying key capabilities for human development.[177] This Article adopts the ten capabilities identified by Nussbaum,[178] noting that while this list is by no means final or conclusive, it represents one of the best attempts to date at identifying such capabilities. Finally, before an individual is completely "used up," there is likely a period during which he is able to produce more benefit to others at the expense of reducing his own capabilities for leading a meaningful life. For example, a young professional might generate more benefits to others (e.g., his employers and family) in the short term by sleeping three hours a day, consuming fast food, and skipping exercise, causing significant harm to his health in the long term. This might be condoned by the first approach, but not the second.

---

173 Sen did note that in practice, one may have to rely on a person's functionings, which is more observable, than capabilities in assessing his well-being. *Id.* at 52 ("Thus, in practice, one might have to settle often enough for relating well-being to the achieved—and observed—functionings, rather than trying to bring in the capability set (when the presumptive basis of such a construction would be empirically dubious).").

174 *Id.* at 39.

175 *Id.* at 49. Sen maintains that capabilities are different from Rawlsian "primary goods" as the latter "may be very imperfect indicators of the freedom that the person really enjoys to do this or be that." *Id.* at 37–38.

176 This approach, however, is also fraught with problems. Any list of functionings deemed essential for an individual is likely to be criticized for being under or over inclusive. Even if a satisfactory list can be agreed upon, there is probably little consensus as to the threshold for each one or set of capabilities/functionings. This is compounded by the fact that the relevant threshold could vary from person to person, depending on an array of factors such as age, gender, health, and social support.

177 SEN, *supra* note 172; Martha Nussbaum, *Capabilities as Fundamental Entitlements: Sen and Social Justice*, 9 FEMINIST ECON. 33, 33–59 (2003).

178 Nussbaum, *supra* note 177, at 41–42.

This approach suggests that whether a case of collective misuse of information can be established depends on two factors: first, the number of people who use an individual's personal information; second, whether the cumulative effect of such use would seriously undermine one or more of the "central human capabilities" that are necessary for leading a flourishing life.[179] The ten "central human capabilities" proposed by Nussbaum include (1) life; (2) bodily health; (3) bodily integrity; (4) senses, imagination and thought; (5) emotions; (6) practical reason; (7) affiliation; (8) other species; (9) play; and (10) control over one's environment.[180]

For the avoidance of doubt, collective misuse of information occurs when a collection of persons uses information about an individual in such a way that undermines one or more of that individual's central human capabilities.

Example: Employment Opportunity

While it is always debatable whether the way a collection of persons uses certain personal information constitutes a "misuse," certain usages are more likely to fall within the scope of "misuse" than others. Using personal information in a way that significantly curtails an individual's employment opportunity serves as a good example. In *The Anti-Bottleneck Principle in Employment Discrimination Law*, Joseph Fishkin documents how personal information such as credit report, criminal record, and unemployment status has been used by employers as screening mechanisms to narrow down the pool of job applicants.[181] He claims that pervasive use of such information constitutes a severe "bottleneck" that prevents people from reaching "a large swath of employment opportunities that open out on the other side."[182] According to Fishkin, both individuals and society benefit from a "more pluralistic opportunity structure."[183] In particular, a more pluralistic opportunity is conducive to human flourishing since it allows people to "experienc[e] the realization of self."[184]

What Fishkin referred to as a "bottleneck" in the opportunity structure is similar to the collective misuse of information problem identified in this Article. Both point to coordination problems in our society that result in undue restraint of individuals' ability to flourish. They are, nevertheless, different in at least two respects. First, Fishkin focuses on the opportunity structure of a society as whole, the shape of which varies

---

179 *Id.*

180 *Id.*

181 Joseph Fishkin, *The Anti-Bottleneck Principle in Employment Discrimination Law*, 91 WASH. U. L. REV. 1429, 1429–1518 (2014).

182 *Id.* at 1449.

183 *Id.* at 1473.

184 *Id.* at 1476 (quoting JOHN RAWLS, A THEORY OF JUSTICE 73 (Rev. ed. 1999)).

from society to society.[185] He invites us to visualize "the numerous opportunities available in any society as being arranged in an *opportunity structure*: a lattice of forking and intersecting paths."[186] Different parts of that structure are "organized in different ways."[187] The paths leading to high elective office, for example, would look very different from those leading to the role of a parent.[188] Reducing "bottlenecks" helps make that opportunity structure "more pluralistic" in the sense that it opens up more paths that lead to various nodes (be it public office or parenthood) in the structure.[189] By contrast, this Article focuses on capabilities that are deemed essential to an individual's flourishing, rather than the overall opportunity structure in a society. This difference is more significant than it may first appear to be.

Firstly, certain collective misuse of information might have a crushing impact on the life of a few individuals, but relatively little impact on the overall opportunity structure of the society. The approach taken in this Article provides greater support for taking steps to reduce this type of misuse. Secondly, focusing on each of the ten capabilities rather than a single metric (i.e., the opportunity structure) might prove to be a more nuanced approach that can be applied to a greater variety of scenarios outside the employment context. Thirdly, it is questionable whether opening up more paths in the opportunity structure is necessarily a desirable goal. Certain nodes in that structure, such as being a sex offender or a terrorist, might better remain connected to as few paths as possible. A theory advocating for a more pluralistic opportunity per se appears incomplete without a complementary theory identifying worthwhile opportunities. By contrast, it is more defendable to claim that any individual should prima facie be entitled to develop capabilities essential to his wellbeing.

b. Second Overuse Analysis: Risk of Wrongful and Harmful Conduct

A second scenario in which a person may be considered "overused" is where he is exposed to an unacceptably high risk of conduct that is considered both wrongful and harmful by society.

Cumulative Risk of Harm

An important feature of risk is that it is cumulative: repeated exposure to activities that are prone to cause harm increases the likelihood

185 *Id.* at 1432.
186 *Id.* at 1471.
187 *Id.*
188 *See id.*
189 *Id.* at 1473.

that harm will materialize.[190] As a result, a group of persons might behave in such a manner that significantly increases the risk that an individual will suffer harm. At the same time, it is possible that not a single person in that group plays a sufficiently decisive role that his withdrawal will significantly decrease the risk of harm. This unique situation has sometimes been analyzed as a "systemic risk," a term which has become well-known since the last financial crisis.[191] Imagine, for example, that one bank, even a major one, did not purchase the risky assets that other banks did. That, alone, probably would not have much effect on preventing a financial crisis.

The same commons problem identified in the previous section is present in the case of systemic risk: a person would have strong incentive to engage in potentially harmful activities since he reaps the full benefit, but does not pay the full cost of his risk-taking. Moreover, since individual withdrawal does not significantly change the likelihood that harm will materialize, each person has little reason to refrain from such activities unilaterally unless a significant number of others promise to do the same.

Example: Ubiquitous Storage and Transfer of Personal Information

Information is the new oil. Every time we disclose our information to a bank, a hotel, a supermarket, or a website, it is most likely that they will store our information for future use.[192] But the flow of information rarely stops at this first point of collection. Within a company, our information may be stored on individual computers or on cloud platforms. It may be downloaded and shared between different members of the company. It might be shared with people in other companies belonging to the same group. It might be sent to third party for research or marketing

---

190 Paul Slovic, *What Does it Mean to Know a Cumulative Risk? Adolescents' Perceptions of Short-term and Long-term Consequences of Smoking*, 13 J. BEHAV. DECISION MAKING 259, 259 (2000).

191 *See, e.g.*, Aaron James, *The Distinctive Significance of Systemic Risk*, 30 RATIO JURIS 239, 240 (2017). ("A risk of harm is created *systematically* when and only when: (1) a group of agents act in a coordinated way (e.g., in a style of capitalism, or subsystem thereof, such as financial markets); (2) in virtue of being so coordinated, the agents' actions, taken together, suffice to significantly raise the chances that someone or other will suffer serious material injury; and yet (3) no single act or single agent's actions, taken separately, significantly changes the probability that harm will occur. If any one of us opts out, the probability of injury will not be lower: the risks in question will be created by the system all the same."). It is worth noting, however, that the definition of "systemic risk" is not entirely clear. Steven L. Schwarcz, *Systemic Risk*, 97 GEO. L.J. 193, 196 (2008).

192 *See, e.g.*, Steven Lewis, *For Banks, Customer Data Is the New King*, EY (Sept. 2013), https://www.ey.com/Publication/vwLUAssets/EY_-_The_upside_of_compliance/$FILE/EY-The-upside-of-compliance-Steven-Lewis.pdf; Julien Dallemand, *What Makes Marriott the Big Data Analytics Leader in Hospitality?*, DATUMIZE, https://blog.datumize.com/big-data-analytics-in-hospitality-marriott-international-case-study (last visited Nov. 9, 2019); Donna Ferguson, *How Supermarkets Get Your Data—and What They Do with It*, GUARDIAN (June 8, 2013), https://www.theguardian.com/money/2013/jun/08/supermarkets-get-your-data.

purposes. According to one UK-based commentator, for any adult, "[a]utomatic backups, log files and emails, plus companies which legally share information with third parties can generate hundreds and thousands of potential copies [of data]," some of which are kept for months or even years.[193]

Each person who retains a copy of our data increases the risk that we fall victim to misconduct such as identify theft. To begin with, it imposes greater risk that criminals will be able to obtain our personal information by hacking into a database containing our information. It has been proven time and time again that even technology giants like Apple and Yahoo cannot avoid the misfortune of being hacked.[194] One might wonder what the chances are that smaller and less tech-savvy companies are able to avoid data breaches.[195] Indeed, some of those companies might not even know that a data breach has taken place for months or years.[196] Moreover, there is also greater likelihood that our information might be accidentally released due to negligence or recklessness of the person storing our information. Some of us might still remember reports about Wells Fargo and Uber accidentally releasing troves of information about their clients and drivers respectively.[197]

Each person who not only stores but also transfers our information to third parties poses additional risks. Each third party to whom information has been transferred is likely to store that information for his own use and/or further transfer that information to others.[198] The same is true for each downstream recipient of that information. As a result, the number of persons storing our information increases exponentially; so is the risk of harm.

---

193 *Individual Customer Data Shared Over 100,000 Times*, DECISIONMARKETING (Sept. 1, 2016), https://www.decisionmarketing.co.uk/news/individual-customer-data-shared-over-100000-times.

194 *Yahoo 2013 Data Breach Hit 'All Three Billion Accounts*,' BBC NEWS (Oct. 3, 2017), https://www.bbc.com/news/business-41493494; Leo Kelion, *Apple Toughens iCloud Security After Celebrity Breach*, BBC NEWS (Sept. 17, 2014), https://www.bbc.com/news/technology-29237469.

195 *See, e.g.*, Gregory Bresiger, *Rise in Data Breaches Wreaking Havoc on Small Businesses: Study*, N.Y. POST (Sept. 28, 2019), https://nypost.com/2019/09/28/rise-in-data-breaches-wreaking-havoc-on-small-businesses-study/.

196 Rich Murphy, *Breach Discovery: How Long Does Detection Take?*, CYBERSHARK (May 10, 2019), https://www.blackstratus.com/breach-discovery-how-long-does-detection-take/.

197 Serge F. Kovaleski & Stacy Cowley, *Wells Fargo Accidentally Releases Trove of Data on Wealthy Clients*, N.Y. TIMES (July 21, 2017), https://www.nytimes.com/2017/07/21/business/dealbook/wells-fargo-confidential-data-release.html; Rich McCormick, *Uber Accidentally Leaks Personal Data for Hundreds of Drivers*, VERGE (Oct. 14, 2015), https://www.theverge.com/2015/10/14/9529095/uber-leaks-personal-information-hundreds-drivers.

198 *See, e.g.*, Yael Grauer, *What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?*, VICE (Mar. 28, 2018), https://www.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection.

Take identity theft as an example. It is perhaps not surprising that the ubiquitous storage and transfer of information has coincided with a rapid increase in incidents of identity theft. Back in 2016, it was estimated that two in five Americans had either been a victim to identity theft or knew someone who had.[199] In 2017, the number of identity theft victims has reportedly risen to 16.7 million, an 8% increase from the previous year and a record high since 2003.[200] As a result, 16.8 billion dollars have been stolen.[201] However, victims of identity theft suffer more than financial loss. According to a recent report by the Identity Theft Resource Center, a large number of the surveyed victims have reported strong negative emotional responses as well as physical reactions.[202] The former includes anger (56%), anxiety (67%), frustration (80%), and fear for financial and physical safety (66% and 24% respectively).[203] The latter includes stress (64.3%), sleep disturbances (48.3%), headaches (33.6%), panic attacks (26.6%), and new physical illnesses (e.g., aches and pains) (23.1%).[204]

To make matters worse, victims of identity theft do not always know the identity of the wrongdoers and therefore unable to recover loss from the latter.[205] They have also had little success suing the entities that have suffered a data breach.[206] Consequently, many of them will have to swallow the loss themselves. Although each individual cannot be completely shielded from occasional misfortune, it may be unreasonable to expect them to tolerate wrongdoing that has such high likelihood of occurrence.

Moreover, identity theft is only one of many harms that are more likely to be suffered by individuals as a result of ubiquitous storage and transfer of information. Such practice also increases the likelihood of occurrence for other misconduct, including discrimination, fraud, as well as collective misuse of information as explained in previous sections. As explained in the next section, it is arguable that actions that collectively facilitate high risk of wrongdoing amount to a form of collective wrong.

---

199 Jessica Dickler, *41 Million Americans Have Had Their Identities Stolen*, CNBC (Oct. 11, 2016), https://www.cnbc.com/2016/10/10/41-million-americans-have-had-their-identities-stolen.html.

200 *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims In 2017*, JAVELIN (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.

201 *Id.*

202 IDENTITY THEFT RES. CTR., IDENTITY THEFT: THE AFTERMATH 2017 10 (2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

203 *Id.* at 11.

204 *Id.* at 12.

205 *See e.g.*, Kelli B. Grant, *Identity Theft Victims: You Might Know the Culprit*, CNBC (July 21, 2015), https://www.cnbc.com/2015/07/21/identity-theft-victims-may-know-the-culprit.html.

206 Solove & Citron, *supra* note 15, at 755.

D. Responsibility for Collective Harm

Even if a person, say John, has suffered significant harm as a result of collective misuse of information, there remains the question of whom should be responsible for his harm. As noted earlier, it is possible that a large number of the persons that contribute to his harm have not breached any social or legal norm in the very context in which each use occurs. In other words, there is no individual misuse of information. Does it entail that none of those individuals should be responsible for John's harm? I will argue that the answer is no.

1. Individual v. Group: Different Standards

To begin with, there is a crucial difference between how we assess individual actions and those of a group. It has been repeatedly observed that we do not apply the same standards when judging individuals and groups. D.E. Cooper highlights the importance of distinguishing "divisible" characteristics from "indivisible" ones.[207] Using Cooper's example, when someone says, "My stamp collection is very old," he may refer to the fact that each of the stamp in his collection is old.[208] Being old is therefore a divisible quality that applies to each member of a group. By contrast, Cooper argues, when someone says that a stew is delicious, he surely does not mean to say that each ingredient making up the stew—garlic, salt, paprika—is individually delicious.[209] Here, being delicious is an indivisible quality that applies to those ingredients collectively.

Joel Feinberg's discussion of contributory group fault is equally instructive.[210] He uses the following example of a train robbery to illustrate how a group of individuals might be blamed despite that each individual is faultless:

> One armed man holds up an entire car full of passengers. If the passengers had risen up as one man and rushed at the robber, one or two of them, perhaps, would have been shot; but collectively they would have overwhelmed him, disarmed him, and saved their property. Yet they all meekly submitted.[211]

In this situation, Feinberg argues, no individual should be faulted for not resisting the robber since only heroes can be expected to act in such

---

207 D.E. Cooper, *Collective Responsibility,* 43 PHIL. 258, 261–62 (1968).

208 *Id.*

209 *Id.* at 262.

210 Joel Feinberg, *Collective Responsibility*, *in* COLLECTIVE RESPONSIBILITY: FIVE DECADES OF DEBATE IN THEORETICAL AND APPLIED ETHICS 53, 61 (Larry May & Stacey Hoffman eds., 1991).

211 *Id.* at 72–73.

circumstances.[212] Nevertheless, "a whole people can be blamed for not producing a hero when the times require it."[213]

Iris Young similarly maintains that we should distinguish individual wrongs from institutional wrongs.[214] She notes that individuals may wrongfully harm other individuals through direct interaction, for example, by acting dishonestly, or abusing one's dominant position.[215] In addition to individual wrongs, Young proceeds to argue:

> We should also ask whether and how we contribute by our actions to structural processes that produce vulnerabilities to deprivation and domination for some people who find themselves in certain positions with limited options compared to others. *It is possible, indeed even likely, that some people can rightly claim that their individual interactions with other people are impeccable, and that at the same time they contribute a great deal to the production and reproduction of structural injustice because of the social position they occupy and the actions they take within it*.[216]

The type of institutional wrong identified by Young is what she refers to as "structural injustice."[217] Young claims that structural injustice exists when:

> social processes put large groups of persons under systematic threat of domination or deprivation of the means to develop and exercise their capacities, at the same time that these processes enable others to dominate or to have a wide range of opportunities for developing and exercising capacities available to them.[218]

To illustrate this concept, she gives the example of a situation in which "there is a lack of availability of affordable housing that forces numbers of people into indecent shelter or makes them vulnerable to homelessness."[219]

Collective misuse of information, as described in this Article, is similar to the structural injustice contemplated by Young in many ways.

---

212 *Id.* at 73.

213 *Id.*

214 *See* IRIS MARION YOUNG, RESPONSIBILITY FOR JUSTICE 73 (2011) ("[W]e should evaluate our actions from two different irreducible points of view: the interactional and the institutional.").

215 *Id.*

216 *Id.* (emphasis added).

217 *Id.*

218 *Id.* at 52.

219 *Id.* at 93.

First, they are both caused by the actions of a large number of people. Second, they are not dependent on proof of individual wrongdoing. Third, they are, as Young points out, not as horrible as systematically perpetrated genocide, but rather can be considered "ordinary" injustice.[220]

Nevertheless, collective misuse of information is different from structural injustice in an important respect. It does not require proof that "large groups of persons" have suffered harm or significant risks of harm. Even if unjustifiable harm is inflicted on only one person, that qualifies as collective misuse of information.

2. Individual Responsibility for Collective Harm

Young draws a helpful distinction between two senses of responsibility. In the first sense, a person is responsible for an action if he is blameworthy for the action or its consequence. Generally speaking, one is blameworthy for an action if he voluntarily performs that action, which causes a harm, and has sufficient knowledge of the consequence of his action.[221] By contrast, in the second sense, responsibility does not entail blame. According to Young, "individuals bear responsibility for structural injustice because they contribute by their actions to the processes that produce unjust outcomes."[222] This responsibility, Young maintains, derives from "participating in the diverse institutional processes that produce structural injustice."[223]

Similar to the case of structural injustice, a person is responsible for collective misuse of information is only responsible in the second sense. However, we have yet to determine what that responsibility entails. According to Young, responsibility for social injustice is a political responsibility, which can be fulfilled in many ways.[224] She has not, however, provided a detailed analysis of those possible measures.

I will argue, more fully in Part III, that this responsibility should include a duty to support the establishment of new institutions that aim at identifying and alleviating collective misuse of information. This in turn justifies the imposition of information tax on certain persons that are likely to contribute more to collective misuse of information due to their position or power.

---

220 *Id.*

221 *Id.* at 97–98 ("The conditions for holding an agent morally responsible are similar to those of legal responsibility: we must be able to show that they are causally connected to the harm in question and that they acted voluntarily and with sufficient knowledge of the consequences.").

222 *Id.* at 105.

223 *Id.*

224 *Id.* at 89.

III. RESOLVING COLLECTIVE MISUSE OF INFORMATION

In this part, I first explain why collective misuse of information cannot be adequately addressed by current approaches to privacy law. Having considered the main causes of collective misuse of information in section B, I will then propose a new solution that supplements existing ones.

A. Inadequacy of Existing Approaches

We are familiar with misuse of personal information by individuals. For instance, people leak secrets, commit identify theft, and publish false statements to undercut a competitor. This section seeks to show that both individual misuse of information and the contextual integrity approach are ill-suited to address collective misuse of information.

1. Individual Misuse of Information

We have shown in Part I that existing privacy laws and regulations focus on what I refer to as individual misuse of information. Under this approach, a person is not liable unless his actions are both wrongful and cause harm or serious offense to others.

However, as explained in Part II, collective misuse of information can exist even if people generally act in accordance with established social and legal norms. It is possible that each person inflicts on an individual a small amount of loss, which appears acceptable in the context that his action takes place. However, the cumulative effect of such loss could reach a tipping point, posing a significant amount of harm on that individual, which is deemed unacceptable by community standards. In other words, collective misuse of information can exist despite the absence of any individual misuse of information.[225] This is because we sometimes judge a group against a different standard than we do an individual.[226] As Joel Feinberg has pointed out, some harms "are ascribable to group faults but not to the fault of every, or even *any*, individual member."[227]

In the case of collective misuse of information, one often encounters a further problem proving that any individual person has caused the victim to suffer harm. For instance, in John's example, a shopping website might argue that even if it does not send any targeted advertisement to John, another website would have done it and, as a result, John would

---

225 Collective misuse of information can also exist in addition to individual misuse of information, causing an individual to suffer a greater amount of harm than he otherwise would have.

226 *See supra* Section II.D.1.

227 Feinberg, *supra* note 210, at 72.

have suffered the same amount of harm.[228] If that is the case, John would have difficulty showing that but for the shopping website's advertisement, he would not have suffered harm. This is in addition to the problem that John would already have in proving that the shopping website has done anything wrong in the first place.

2. Recognizing More Types of Privacy Harm

Solove and Citron have argued in favor of extending the scope of privacy harm to include risks of harm. Their case study reveals that, while courts tend to award damages where a data breach lead to identity theft, most courts have been reluctant to recognize harm in the absence of "proof of physical harm or financial loss."[229] Solove and Citron in turn advocate for judicial recognition of two new types of data breach harms: (1) increased risk of suffering a legally cognizable harm (such as identity theft) and (2) anxiety over a data breach.[230]

While Solove and Citron have made a strong case for recognizing risk of harm as harm, their analysis still focuses on the imposition of risk by a defendant on one or more plaintiffs. As a result, their analysis sheds relatively little light on the type of harm discussed in this Article: that is, harm caused by multiple persons.

3. Contextual Integrity

Helen Nissenbaum argues that the right to privacy is the "right to *appropriate* flow of information," that is, flow of information that complies with context-relative informational norms.[231] Those are norms that govern "the flow of personal information . . . from one party to another, or others."[232] These norms vary according to the context in which information is transmitted (e.g., a workplace or courtroom); the type of infor-

---

228 Shelly Kagan, *Do I Make a Difference?*, 39 PHIL. PUB. AFF. 105, 129–30 (2011). This is similar to the problem of "imperceptible harm" that Shelly Kagan discussed and dismissed in her article, *Do I Make a Difference?*. *Id.* at 130. The troubling position is the following:

> If my act makes only an imperceptible difference, and that difference does not itself constitute a harm, then even had I acted differently the results would have been no better. In such a case, (individualistic) consequentialism seems incapable of condemning my act, even though when enough of us act in this way the results are very bad indeed.

Id. Kagan denies the existence of such problems. According to her, all problems of imperceptible harm are triggering cases, that is, one of n people triggers a bad result. Even if a person does not know whether he is one of n people, he "can still know that the *expected* utility of [his] act is negative." *Id.* at 129. This latter observation is highly questionable. *See* Mark Bryant Budolfson, *The Inefficacy Objection to Consequentialism, and the Problem with the Expected Consequences Response*, 176 PHIL. STUD. 1711, 1721–22 (2019).

229 Solove & Citron, *supra* note 15, at 755.

230 *Id.* at 756–74.

231 NISSENBAUM, *supra* note 1, at 127.

232 *Id.* at 140.

mation transmitted; and the social roles played by the sender, recipient, and subject of that information.[233] Contextual integrity is "preserved when informational norms are respected and violated when informational norms are breached."[234]

Nissenbaum briefly discusses the problem that we refer to as collective misuse of information at the end of her book, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*.[235] "If so many of the individual incursions, taken by themselves, cause only tiny, even imperceptible breaches . . . " she asks, "how is it possible to address the big, truly worrisome totality with policies targeted to any one of these?"[236] She contends that this problem can be resolved by the framework she has proposed. According to Nissenbaum, established information norms generally embody the values and purposes of the contexts in which those their norms are developed.[237] As a result, those norms are sufficiently robust to account for the indirect impact of any questionable action, thereby preventing collective misuse of information from arising in the first place.[238]

This Article agrees with Nissenbaum's assertion that context-specific informational norms can alleviate collective misuse of information to a certain extent. However, this Article questions the adequacy of her solution. One of the main aims of this Article is to show that practices which appear to comply with informational norms in specific contexts might nevertheless collectively cause harm to an individual. One might argue in response that there are contexts of varying specification, one nested within another. Even if a practice seems innocuous in a specific context, it might turn out to be questionable if one takes a step back to examine the more general, higher-level, context.[239] This may be true. However, it is worth noting that the more general a context is, the more difficult to identify the core value or purpose of that context, and therefore, the harder to determine whether a practice complies with the infor-

---

233 *Id.* at 141.

234 *Id.* at 140–41.

235 *Id.* at 241–43.

236 *Id.* at 242.

237 *Id.* at 138.

238 *Id.* at 242–43 ("This problem is addressed in the framework of contextual integrity by contexts themselves. Entrenched informational norms generally embody a scheme of settled informational practices roughly oriented around the values, ends, and purposes of a context; contexts generally are the structured social systems that have evolved to manage and accomplish aspects of social life recognized as fundamental in a given society. This scheme imbues each questionable action and system with a meaning that extends far beyond its immediate reach, its direct impact, taken alone. It is the robustness of the social structure of contexts and the efficacy of their respective informational norms that stop the slide down the slope and prevent a society from throwing away privacy in tiny bits.").

239 *Id.* at 136. Nissenbaum specifically refers to nesting as one possible relationship between different contexts.

mational norms of that context. Nissenbaum's theory is arguably most useful when applied to highly contextual circumstances.

Moreover, it may be too idealistic to expect informational norms to resolve all coordination problems. Similar to the concept of market failure, there could be "norm failure" which requires judicial or regulatory intervention.

B. Why Does Collective Misuse of Information Occur?

1. Incentive Mismatch

Joshua Fairfield and Christoph Engel note that privacy shares the same incentive structure as other public goods such as clean air and safety, and therefore suffers from the same problems.[240] They assume that some individuals will disclose information about themselves or others if they believe that the direct benefit of such disclosure to them outweighs the direct cost, even if the total cost of the disclosure to the society is greater than the direct benefit to himself.[241] They then argue that since individuals have reason to believe that other people will choose to disclose information, were they faced with the same choice, they are less likely to choose the privacy preserving option at their own expense.[242]

It is submitted that similar incentive structure exists not only where people decide whether to disclose a piece of information to their benefit, but also where people decide what to do with the information they have collected. For example, when an employer decides whether to stipulate that all applicants must possess tertiary education for a job that clearly does not require such education, she makes the following calculation: "If I use that requirement to screen job applications, the list of applications that I need to review will shorten significantly. The amount of time I will save is a direct benefit to me." Stipulating such a requirement might im-

---

240 Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 391 (2015) ("Luckily, privacy is by no means the only public good. Clean air, safety, roads, and the common defense all share the same incentive structure.").

241 *Id.* at 423 ("Translated to privacy, the public-goods model assumes that at least some individuals calculate the following way: If I disclose information, I will receive a private benefit-access to an online site or service, for example. This imposes a cost on me, based on the personal information I have given up, and it imposes a cost on everyone because I have contributed to the overall lack of privacy in the culture. Yet as long as the sum of my direct costs and my share of the social costs (resulting from my own release of private information) is less than the private benefit I gain, I will choose to give up information to access the site or service.").

242 *Id.* at 425 ("Individuals who face the social dilemma of privacy face three strong pressures to defect even if they are inclined to cooperate: they realize that their individual efforts will only cost them; that others will likewise defect over time; and that the development of technology tends toward ever-greater intrusions on privacy. No wonder, then, that even the most privacy-minded consumers may eventually defect.").

pose a cost on job applicants who do not satisfy this criterion—they might have to look further and longer for a job or to accept a job that pays less. It may also impose a cost on society since the job can be adequately performed by someone without any tertiary education: if all employers impose more stringent requirements than what they actually need, job seekers are likely to pursue more education than they need, which will eventually result in a society's over-investment in education. Nevertheless, the employer is incentivized to impose that requirement because the direct benefit to her (i.e., saving her time as well as any potential benefit of having an overqualified employee) outweighs the direct cost. She does not bear the cost she imposes on potential job seekers and only bears a fraction of the cost to the society. Further, she has greater incentive to impose such requirement if she expects her competitors will do the same. She might be at a competitive disadvantage if other people are able to hire overqualified people through a less time-consuming process.

2. Ignorance: A Second-order Collective Action Problem

As Ostrom points out, even if a new set of rules can resolve or alleviate an existing collective action problem, the supply of such new rules poses a "second-order collective dilemma" since the new rules are "subject to the very incentive problems [they are] supposed to solve."[243] One of Ostrom's key findings is that an important first step towards overcoming a collective action problem is to determine precisely when and how a common pool resource is overused.[244]

A similar ignorance problem is present in the case of collective misuse of information. More often than not, a person using another's personal information might know the direct costs she imposes on an individual, but not the total amount of harm that her action, when combined with the actions of a large number of people, might inflict on that individual. Nor can she be expected to know the full consequence of her action for a number of reasons. Firstly, each person probably has no way of knowing the identity of other persons who also impose costs on the same individual over an extended period of time. Secondly, the effect of one person's action on an individual might interact with that of another action. As our hypothetical example has shown, John's shopping spree can potentially affect his ability to obtain affordable loans, insurance, or even employment. Thirdly, there is uncertainty over how each individual would respond to a particular set of circumstances. As a result, it may be fair to conclude that, in John's case, a shopping website probably does

243 OSTROM, *supra* note 150, at 103 (quoting Robert H. Bates, *Contra Contractarianism: Some Reflections on the New Institutionalism*, 16 POL. SOC'Y 387, 395 (1988)).

244 OSTROM, *supra* note 150, at 33.

not know and cannot be expected to know that its advertisement might be one among many incidents that eventually lead to his plight.

The difficulty of identifying cumulative harm is compounded by the fact that each contributor of a collective misuse of information has little incentive to investigate the cumulative harm of her action. If a contributor does investigate, she might have reason to believe that her action, when combined with others, can cause significant harm to one or more individuals. As a result, those individuals might be able to argue that the contributor's knowledge renders her complicit in a series of activities that cause harm to them, and they may seek compensation on that basis. In other words, the contributor has little to gain from this additional knowledge, but everything to lose.[245]

3. Disagreements Over What Constitutes a Collective Misuse of Information

As noted in Part II, it is relatively easier to determine whether an object, such as a lake or a pasture, has been overused. The question is more complicated for two reasons when the relevant common pool resource is human. First, there is no clear consensus over the minimum set of resources or capabilities that each individual deserves to enjoy. Second, victims of collective misuse of information may have partially contributed to their own misfortune, but it is difficult to determine with any accuracy to what extent each individual victim is responsible.

C. Information Tax

1. Justifying an Information Tax

A well-designed information tax can be an effective way to resolve some of the problems posed by collective misuse of information. As explained in the previous section, an important impediment to resolving collective misuse of information is a knowledge gap: persons who collectively cause harm to an individual may not know the full extent of the potential harm and benefit of their action.[246] Without this information, it would be difficult for members of a collective or for external regulators to design rules to regulate harm-causing conduct. An information tax can

---

245 As Steven Shavell noted in his article, *Liability for Harm versus Regulation of Safety*, a person engaging in risky behavior might not possess accurate information about the severity of those risks because such information is not obvious and the person does not have sufficient incentive to acquire that information. Steven Shavell, *Liability for Harm versus Regulation of Safety*, 13 J. LEGAL STUD. 357, 360 (1984) ("In certain contexts information about risk will not be an obvious by-product of engaging in risky activities but rather will require effort to develop or special expertise to evaluate. In these contexts[,] a regulator might obtain information by committing social resources to the task, while private parties would have an insufficient incentive to do this for familiar reasons.").

246 *See supra* Section II.B.2.

help provide the necessary financial resources to establish institutions that seek to fill that knowledge gap.

Moreover, taxation can provide a useful source of compensation to victims of collective misuse of information. Even if certain activities turn out to cause more good than harm overall, it does not follow that the persons performing those activities have no responsibility to remedy the associated harm. As we have argued, each person, as member of a community, has a duty to participate in minimizing group wrongs.[247]

Further, as Steven Shavell has observed, taxation is sometimes more appropriate than harm-based sanction or regulation to control undesirable behavior.[248] Using pollution as an example, Shavell argues that harm-based sanction is not well suited for this problem because "it may be difficult to identify and link harm caused by pollution to responsible parties."[249] Moreover, since the cause of pollution is complex and the harm can take years to eventuate, polluters are often able to escape sanction.[250] On the other hand, Shavell points out that effective regulation requires too much information to enact and implement.[251] The regulator must not only know "the expected harm due to the activity but also the benefit from the activity" in order to conduct a cost-benefit analysis and to determine whether intervention is socially desirable.[252] By contrast, a corrective tax, which Shavell defines as "a tax equal to the expected harm caused by an activity," requires less information since the regulator only has to know "the expected harm due to the [harmful] activity."[253]

Although Shavell focuses on a corrective tax, his observations are relevant for present purposes as well. As our discussion has shown, collective misuse of information shares many characteristics with pollution. It is often difficult to attribute an individual's harm to any specific person since a large number of people contribute to that harm. Similar to pollution, the harm of collective misuse of information can also take years to develop, making it more difficult to identify wrongdoers. Moreover, many of the people contributing to that individual's harm might not be perceived to have done anything wrongful in their specific contexts. Even if they have committed a wrong, it may not be cost effective for a victim to pursue a large number of wrongdoers, each causing a small amount of loss. As a result, harm-based sanction is often ineffective.

---

247 *See supra* Section II.D.2.

248 Steven Shavell, *The Optimal Structure of Law Enforcement*, 36 J.L. ECON. 255, 284–85 (1993).

249 *Id.* at 284.

250 *Id.*

251 *Id.* at 285.

252 *Id.*

253 *Id.* at 284–85. Shavell also cautions that taxation is not a panacea for all problems and highlights the need to take into account the cost of enforcing a tax. *Id.* at 85.

For the avoidance of doubt, the proposed information tax is not meant to be a panacea for all problems that arise in the big data era. Many times, imposing liability for individual misuse of information or requiring recipients to disclose how personal information is collected and used can be more effective at curbing conduct that is clearly undesirable.[254]

2. Designing an Information Tax

We have suggested, following Iris Young, that persons who contribute to collective misuse of information are responsible for that misuse.[255] We have further argued that taxation can be an effective means to hold those persons responsible.[256] Nevertheless, designing an effective information tax system can be a challenging task. Recently, Austria has reportedly attempted, but failed, to introduce value added tax on big data transactions due to the "complications of assigning a fixed value to such transactions."[257]

In the following sections, I sketch a proposal for an information tax that is grounded in people's responsibility to alleviate collective misuse of information.

a. Who to Tax

As discussed in Part II, collective misuse of information involves a large number of people, and one person can, knowingly or unknowingly, contribute to multiple incidents of misuse at the same time. At first sight, our discussion appears to suggest that almost all persons should be liable for information tax since we all, at one time or another, use other individuals' information at their expense. However, imposing an information tax on every person can be both administratively costly and unfair. Some individuals might play such a minimal role in causing collective misuse of information that the costs of collecting information tax from them outweigh the amount of tax recoverable from them.

Therefore, it is submitted that the information tax should target persons who play an instrumental role in producing collective misuse of information. These persons may fall into the category of information user, information transmitter, or both.

---

254 For a discussion of the limits of corrective tax, see generally Victor Fleischer, Essay, *Curb Your Enthusiasm for Pigovian Taxes*, 68 VAND. L. REV. 1673 (2015).

255 *See supra* Section II.D.2.

256 *See supra* Section III.C.1.

257 Saadia Madsbjerg, *It's Time to Tax Companies for Using Our Personal Data*, N.Y. TIMES (Nov. 14, 2017), https://www.nytimes.com/2017/11/14/business/dealbook/taxing-companies-for-using-our-personal-data.html.

i. Information Users

A person may occupy such an important position in the social structure that an adverse decision made by that person has greater propensity to cause harm to another individual. Only persons that exert a significant amount of influence over other individuals should be subject to an information tax.

The amount of influence a person exerts over others can be determined by how essential the types of goods and services offered by that person are. For example, a bank refusing to lend money to John is more likely to cause him harm than a grocery refusing to sell him a carrot. The amount of influence also depends on that person's market share. A landlord renting out a bedroom in her own house is less influential than a professional rental company.

In other words, there should be an information tax exemption for small businesses and for companies in less essential industries in relation to their use of personal information in decision-making.

ii. Information Transmitters

Information transmitters are different from information users in an important aspect: they do not directly use personal information to make decisions, but rather enable others to use information for such purposes (often for a fee). A prime example of information transmitters is the data brokers mentioned in Part I, which sell personal information that they have collected from various sources. Another example would be various platforms such as Facebook and Google AdWords, which enable advertisers to capitalize on the wealth of personal information they have collected.[258]

These intermediaries are ideal candidates of information tax for several reasons. First, by allowing personal information to be used and reused by a large number of persons, they significantly increase the likelihood that third-party usage might produce significant cumulative harm or risk of harm over an extended period of time. Second, these intermediaries often reap lucrative profits during the process. It is estimated that data brokers alone would generate $250 billion in revenue by 2018.[259]

---

[258] Roomy Khan, *Facebook: Piñata, Scapegoat and Villain*, FORBES (Nov. 30, 2018), https://www.forbes.com/sites/roomykhan/2018/11/30/facebook-pinata-scapegoat-and-villain/#73bcec139f93.

[259] Madsbjerg, *supra* note 257.

b. Tax Rate

While determining the optimal amount of tax to be levied requires further investigation, three preliminary observations can be made. First, the main purpose of the information tax is to provide funds to establish the necessary institutions for identifying social structures that are likely to lead to collective misuse of information and to provide compensation to victims. Consequently, the amount of tax to be levied should correlate with the amount of estimated expenses each year.

Second, information transmitters appear to play a more structurally significant role in producing collective misuse of information than a mere information user.[260] As a result, it may be appropriate to impose a higher tax on the former.

Third, for some companies, even a small amount of tax on revenue can generate a significant amount. Take data brokers as an example: a 0.8% tax on revenue would probably yield $2 billion annually.[261] It is also worth noting that a tax on revenue is arguably more appropriate than a tax on profit because many technology firms take years to turn a profit.[262]

CONCLUSION

This Article draws attention to the need to focus on collective, as opposed to individual, misuse of information in the big data era. Responsibility for collective misuse of information derives from our responsibility as members of a community to identify and remedy group wrongs. It in turn provides a basis for imposing information tax on persons that make nontrivial contributions to collective misuse of information.

260 *See supra* Part II.

261 Madsbjerg, *supra* note 257.

262 *See* Kevin Roose, *The Entire Economy Is MoviePass Now. Enjoy It While You Can.*, N.Y. TIMES (May 16, 2018) https://www.nytimes.com/2018/05/16/technology/moviepass-economy-startups.html.