A THEORY OF GROUP PRIVACY

*Anuj Puri**

* PhD candidate at the St. Andrews and Stirling Graduate Program in Philosophy (SASP) at the University of St. Andrews. This Article is dedicated to the memory of my PhD supervisor Prof. Katherine Hawley. I am grateful to Prof. Kirstie Ball and Prof. Rowan Cruft for guiding and supporting my research. For helpful discussion and comments on this Article, I am grateful to Abhijeet Awasthi, Kirstie Ball, Swethaa Ballakrishnen, Rowan Cruft, Mark Dsouza, Wouter Schmit Jongbloed, Petros Mavroidis, Colin Mclean, Akhil Puri, Nidhi Sahay, Abhishek Singhal and Anuj Tyagi. Early drafts of this Article were presented at the 2nd Transatlantic Conference on Data & Ethics, University of Vienna, 2019 and the Bodaken Philosophy Symposium, Colorado State University, 2019. I am grateful to the participants at both the conferences for their feedback, particularly Bruce Bodaken, Moti Gorin, Norman Spaulding, and James Williams. I am grateful to the team at the Cornell Journal of Law and Public Policy for their editorial guidance and support. The errors are my own.

"To know what a man is, you must not take him in isolation. . . The mere individual is a delusion of theory."
F.H. Bradley, ETHICAL STUDIES, 173–74 (1876)

In the age of Big Data Analytics and Covid-19 Apps, the conventional conception of privacy that focuses excessively on the identification of the individual is inadequate to safeguard the individual's identity and autonomy. An individual's autonomy can be impaired and their control over their social identity diminished, even without infringing the anonymity surrounding their personal identity. A century-old individualistic conception of privacy that aimed at safeguarding a person from unwarranted social interference is incapable of protecting their autonomy and identity when they are targeted on the basis of their interdependent social and algorithmic group affiliations. In order to overcome these limitations, in this Article, I develop a theoretical framework in the form of a triumvirate model of the group right to privacy (GRP), which is based on privacy as a social value (P_v). An individual has an interest in protecting their social identity arising out of their participation in social groups. The panoptic sorting of individuals by Big Data Analytics for behavioral targeting purposes gives rise to epistemic bubbles and echo chambers that impede the formation of an individual's social identity. I construct the formulation of GRP_1 to protect an individual's interest in their social identity and their socially embedded autonomous self. Thereafter, I emphasize an individual's right to informational self-determination and against algorithmic grouping in GRP_2. Lastly, I highlight instances where

GRP_3 entitles an organized group to privacy in its own right. I develop a Razian formulation to state that Big Data Analytics's constant surveillance and monetization of human existence is an infringement of individual autonomy. The violation of GRP subjects an individual to behavioral targeting (including hyper-targeted political advertising) and distorts their *weltanschauung*, or worldview. As regards Covid-19 Apps, I assert that the extraordinary circumstances surrounding the pandemic do not provide an everlasting justification for reducing an individual's identity to a potential disease carrier. I argue that the ambivalence regarding existence of surveillance surrounding an individual's social identity can leave them in a perpetual state of simulated surveillance (simveillance). I further assert that it is in the long-term best interests of the Big Tech corporations to respect privacy.

In conclusion, I highlight that our privacy is not only interdependent in nature, but it is also existentially cumulatively interlinked. It increases in force with each successive protection. The privacy challenge posed by Covid-19 Apps has helped us realize that while limited exceptions to privacy may be carved out in grave emergencies, there is no moral justification for round-the-clock surveillance of an individual's existence by Big Data Analytics. Similarly, the threat to privacy posed by Big Data Analytics has helped us realize that privacy has been wrongly focusing on the distinguishing aspects of the individual. It is our similarities that are truly worth protecting. In order to protect these similarities, I formulate the concept of mutual or companion privacy, which counterintuitively states that in the age of Big Data Analytics, we have more privacy together rather than individually.

INTRODUCTION

In July 1890, Wilde presciently warned "*[t]o define is to limit.*"[1] Later that year, in December 1890, Warren and Brandeis defined the right to privacy as "*the right to be let alone.*"[2] Over the course of the last 130 years, as the nature of privacy violations has shifted from social interferences to algorithmic inferences, the limitations of the traditional conception of privacy have become exposed. In the age of Big Data Analytics[3] and Covid-19 Apps, ("a mobile phone app that captures 'proximity events'—events in which two mobile phones have been close enough

---

1 OSCAR WILDE, THE PICTURE OF DORIAN GRAY 251 (1981).

2 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (articulating the right to privacy as "the right to be let alone." (emphasis added)).

3 PHILIP RUSSOM, TDWI BEST PRACTICES REPORT: BIG DATA ANALYTICS 56 (2011) (noting that "the three Vs of big data (volume, variety, and velocity) constitute a comprehensive definition" of Big Data" and "big data analytics is where advanced analytic techniques operate on big data sets.").

for sufficient time for the risk of infection to be high[.]"),[4] the conventional conception of privacy that focuses excessively on identification of the individual is inadequate to safeguard the individual's identity and autonomy.[5] As Barocas and Nissenbaum point out, "[e]ven when individuals are not 'identifiable', they may still be 'reachable', may still be comprehensibly represented in records that detail their attributes and activities, and may be subject to consequential inferences and predictions taken on that basis."[6] Further, the interdependent nature of our networked existence means that for data processing purposes we unconsciously belong together in a social or algorithmic group.[7] The information pertaining to one individual can be processed to negatively impact the autonomy of other members belonging to the said group.[8] Hence, the privacy violation of one member of this social or algorithmic group impacts all the members of the group.[9] Search engines reinforcing racism,[10]

---

4 Michael J. Parker, Christophe Fraser, Lucie Abeler-Dörner, & David Bonsall, *Ethics of Instantaneous Contact Tracing Using Mobile Phone Apps in the Control of the COVID-19 Pandemic*, 46 J. MED. ETHICS 427, 427 (2020).

5 Anna Johnston, *Individuation: Re-Imagining Data Privacy Laws to Protect against Digital Harms*, 6 BRUSSELS PRIVACY HUB WORKING PAPER 12 (2020) ("A person does not need to be identified in order for their autonomy to be undermined or their dignity to be damaged.").

6 *See* Solon Barocas & Helen Nissenbaum, *Big Data's End Run around Anonymity and Consent*, *in* PRIVACY, BIG DATA AND THE PUBLIC GOOD FRAMEWORKS FOR ENGAGEMENT 45 (Julia Lane, Victoria Stodden, Stefan Bender, & Helen Nissenbaum eds., 2014) (focusing on mitigating the conflict between big data and ethical values).

7 Karen Levy & danah boyd, *Networked Rights and Networked Harms* 1–2 (Privacy Law School Conference, Working Paper 2014) (exploring "two interwoven concepts of 'networked rights' and 'networked harms'"); *see also* Lanah Kammourieh et al., *Group Privacy in the Age of Big Data*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 37, 56–62 (Linnet Taylor, Luciano Floridi, & Bart van der Sloot eds., 2017) (discussing how to secure group privacy via traditional levers of power and better data security, management, and literacy).

8 Linnet Taylor, Luciano Floridi, & Bart van der Sloot, *Introduction: A New Perspective on Privacy*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 1, 5–6 (Linnet Taylor, Luciano Floridi, & Bart van der Sloot eds., 2017) (addressing the concerns arising from new data analytical technologies with regard to collectives); Barocas & Nissenbaum, *supra* note 6, at 45; *see also* Solon Barocas & Karen Levy, *Privacy Dependencies*, 95 WASH. L. REV. 555, 583 (2020) (demonstrating how different types of privacy dependencies can raise different normative concerns).

9 Bernadette Kamleitner & Vince Mitchell, *Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringements*, 38(4) J. PUB. POL'Y & MARKETING 433, 435 (2019). ("The phenomenon of interdependent privacy infringements arises through the intertwined nature of human beings in society"); *see also* Mathias Humbert, Benjamin Trubert, & Kévin Huguenin, *A Survey on Interdependent Privacy*, 52 ACM COMPUTING SURVEYS 1, 2 (2020) (summarizing and analyzing research on interdependent privacy risks).

10 SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 26 (2018) ("Marginalized and oppressed people are linked to the status of their group and are less likely to be afforded individual status and insulation from the experiences of the groups with which they are identified.").

algorithms discriminating in employment on the basis of gender,[11] algorithms unfairly downgrading student marks on the basis of schools' results in previous years,[12] and consumer identity getting compromised on the basis of shopping patterns[13] are all examples of automated assault on an individual's autonomy and identity on the basis of their membership in social and algorithmic groups. In order to address the limitations of the conventional conception of privacy, in this Article, I shift the focus of privacy from identification to identity formation[14] and from the individual to the group.[15] Using this paradigm shift, I construct a theoretical framework that is rooted in privacy as a social value (P_v).[16] The theoretical model aims to counter the various privacy threats that we face at an individual and group level in a hyperconnected world by developing an interlinked mechanism to protect the interdependent nature of our mutual privacy.

The aforementioned limitations of the Individual Right to Privacy (IRP) and the targeting of the individual on the basis of their group mem-

---

11 *See* Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, REUTERS (Oct. 10, 2018, 7:04 PM), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

12 James Clayton & Zoe Kleinman, *The Algorithms That Make Big Decisions About Your Life*, BBC (Aug. 17, 2020), https://www.bbc.co.uk/news/technology-53806038.

13 Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp&mtrref=undefined&gwh=6C719A5602C48362622D5774F1C72C97&gwt=pay&assetType=REGIWALL.

14 *See* Mireille Hildebrandt, *Privacy and Identity*, *in* PRIVACY AND THE CRIMINAL LAW 43, 44 (Erik Claes, Anthony Duff, & Serge Gutwirth eds., 2006) (emphasizing the role of privacy in identity building). Hildebrandt asserts that privacy is not merely about access to personal information, but also about identity-building. *Id.* By highlighting privacy's role in identity formation, I seek to protect an individual's social identity that arises out of their participation in social groups. Michael A. Hogg, *Social Identity Theory*, *in* UNDERSTANDING PEACE AND CONFLICT THROUGH SOCIAL IDENTITY THEORY: CONTEMPORARY GLOBAL PERSPECTIVES 3, 6 (Shelley McKeown, Reeshma Haji, & Neil Ferguson eds., 2016) (describing the core tenets of social identity theory).

15 For shifting ontology of privacy *see* Kammourieh et al., *supra* note 7, at 43.

16 Privacy is not only an individual right but also a social value. Regan suggests three bases for the social importance of privacy:

> First, privacy is a common value in that all individuals appreciate some degree of privacy and have some shared perceptions about privacy. Second, privacy is a public value in that it has worth broadly to all aspects of the democratic political process. And third, privacy is a collective value in that technology and market forces are making it hard for any one person to have privacy without all persons having a similar minimum level of privacy.

Priscilla M. Regan, *Privacy and the Common Good: Revisited*, in SOCIAL DIMENSIONS OF PRIVACY INTERDISCIPLINARY PERSPECTIVES 50, 50 (Beate Roessler & Dorota Mokrosinska eds., 2015) (reflecting on the philosophical developments in privacy). *See generally*, PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 212–45 (1995). In my theoretical model, P_v serves as ground for the individual and group formulations of privacy.

berships have given rise to calls for the Group Right to Privacy (GRP).[17] However, GRP since its initiation has been fighting for validation and independent existence.[18] Critics have questioned both the existence of the group[19] and its ability to bear rights.[20] So, as things stand today, while there is consensus regarding limitations of the present conception of IRP, debate rages on over whether GRP is the answer to those limitations.

This Article seeks to resolve this debate by exploring GRP on the dual lines of the individual's right as a member of a group and the right of the group itself.[21] I further take the position that the limitations of the conception of individual privacy cannot be removed without erasing the limitations on the conceptualization of the individual.

As regards the dual construction of GRP, Bloustein defined group privacy as "a form of privacy that people seek in their associations with others."[22] For Bloustein, group privacy was "an attribute of individuals in association with one another within a group, rather than an attribute of the group itself."[23] However, *ordinarily* a group right is considered to be the right of the group rather than that of the members of the group.[24] The emphasis while determining the bearer of the right is on the subject of

---

17 *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967). Westin defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." *Id.*

18 *See* EDWARD J. BLOUSTEIN, INDIVIDUAL & GROUP PRIVACY 125 (2d ed. 2003) (considering group privacy as an extension of individual privacy).

19 The determination of a group is extremely difficult in cases of mass surveillance and profiling. When group members are not even conscious of each other's existence, can we say that the group exists? Recent scholarship in the area tries to overcome this problem by terming such groups either as "passive groups" or saying that these groups are designed by level of abstraction. *See* Kammourieh et al., *supra* note 7, at 38-39; *see also* Luciano Floridi, *Group Privacy: A Defence and an Interpretation*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 83, 84 (Linnet Taylor, Luciano Floridi, & Bart van der Sloot eds., 2017) (identifying and resolving problems affecting the plausibility of group privacy).

20 Peter Jones, *Group Rights*, *in* STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta ed., 2016).

21 *See* Rowan Cruft, S. Matthew Liao, & Massimo Renzo, *The Philosophical Foundations of Human Rights: An overview*, *in* PHILOSOPHICAL FOUNDATIONS OF HUMAN RIGHTS 1, 29 (Rowan Cruft, S. Matthew Liao, & Massimo Renzo eds., 2015) (providing an overview of the philosophical foundations of human rights). The authors state that there can be two types of group human rights:

> We can distinguish two types of group human right. One is a human right held by an individual on the basis of [their] membership of a particular group. Examples include the distinctive rights one holds as a woman, a child, or a member of a minority group. The second type is a human right held by a group. An example is a people's right to self-determination.

Id. (internal citations omitted).

22 Bloustein, *supra* note 18, at 124.

23 *Id.*

24 Jones, *supra* note 20.

the right and not the object of the right.[25] This raises a conundrum for GRP. If group privacy is an attribute of the group members but not the group, and group right is the right of the group but not the group members, then what is GRP? Is it a right of the group or the members or both? The dual construction of GRP that I invoke to resolve this conundrum is consistent with the existing exceptions to the dichotomy between group rights and individual rights. Kymlicka has favored the recognition of group-differentiated rights, which are the rights that vest on the basis of an individual's membership in a social group.[26] Group-differentiated rights are granted to members of a social group in order to remedy inequities.[27] Macdonald further has defined group rights as rights individuals enjoy on the basis of their membership in a group.[28] He specifically emphasizes the rights arising out of group membership that are integral to the individual's identity.[29] While it is beyond the scope of this Article to articulate a general theory of group rights, my formulation of group rights is especially pertinent from privacy's perspective, where the distinction between individual interest and group interest is not as sharply delineated as some other rights. Big Data Analytics may analyze an individual's attributes to draw inferences about the group that they belong to and vice-versa, an individual may be targeted on the basis of their membership in a group. Hence, the dual formulation of the GRP is justifiable.

As regards limitations on the conception of the individual, historically when it comes to identity, privacy concerns have been overtly focused on protecting the personal identity much to the neglect of social identity.[30] Similarly, the relationship between privacy and autonomy was classically construed as aimed at keeping the liberal self outside the purview of social gaze rather than protecting the socially embedded autono-

---

25 *See* Peter Jones, *Human Rights, Group Rights, and People's Rights*, 21 HUM. RTS. Q. 80, 82–83 (1999) (marking that what differentiates a right from a group right is who holds the right in question).

26 WILL KYMLICKA, MULTICULTURAL CITIZENSHIP: A LIBERAL THEORY OF MINORITY RIGHTS 6 (Oxford University Press, 1996) ("A comprehensive theory of justice in a multicultural state will include . . . certain group-differentiated rights or 'special status' for minority cultures.").

27 *See* Eric J. Mitnick, *Three Models of Group-Differentiated Rights*, 35 COLUM. HUM. RTS. L. REV. 215, 215 (2004) (discussing examples of inequities remedied by group-differentiated rights).

28 Ian Macdonald, *Group Rights in South Africa: A Philosophical Exploration*, 15 POLITIKON 19, 24–25 (1988); *see also* Seumas Miller, *Group Rights Revisited*, 33 PHIL. PAPERS SPECIAL ISSUE 187, 192 (2004) (expounding on Macdonald's theory that group rights are rights individuals have by virtue of belonging to some social group).

29 Macdonald, *supra* note 28, at 25.

30 *See* Regan, *supra* note 16, at 53–55 (detailing how scholarship at the beginning of the 20th century defined privacy primarily through an individualistic lens). *See also* Richard Baskerville, Tawfig Alashoor & Ruilin Zhu, *Rethinking the Privacy and Identity Relationship* 1 (2014), https://www.nitrd.gov/cybersecurity/nprsrfi102014/Baskerville_Alashoor_Zhu.pdf.

mous self.[31] I assert that these limited accounts of identity and autonomy[32] have given rise to a false duality between the traditional conception of IRP and what is presently considered to be GRP. This false duality can be eliminated by protecting an individual's interest in their socially embedded, autonomous self and their social identity arising out of their membership in social groups (GRP_1).[33] Big Data Analytics's panoptic sorting[34] of individuals for behavioral targeting[35] purposes gives rise to epistemic bubbles[36] and echo chambers[37] that impede the

---

31 As per Cohen,

> The liberal self who is the subject of privacy theory and privacy policymaking does not exist. . . the self who is the real subject of privacy law and policy is socially constructed, emerging gradually from a preexisting cultural and relational substrate. For this self, privacy performs a function that has nothing to do with stasis. Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable. It protects the situated practices of boundary management through which the capacity for self-determination develops.

Julie E. Cohen, What privacy is for, 126 Harv. L. Rev. 1904, 1905 (2013). *See also* Dorota Mokrosinska, *Privacy and Autonomy: On Some Misconceptions Concerning the Political Dimensions of Privacy*, 37 L. & PHIL. 117, 121–22 (2018) (noting the shift in privacy discourse from detached liberal self to socially embedded self).

32 My understanding of autonomy is guided by Raz's pronouncement,

> "If a person is to be maker or author of his own life then he must have the mental abilities to form intentions of a sufficiently complex kind, and plan their execution. These include minimum rationality, the ability to comprehend the means required to realize his goals, the mental faculties necessary to plan actions, etc. For a person to enjoy an autonomous life he must actually use these faculties to choose what life to have. There must in other words be adequate options available for him to choose from. Finally, his choice must be free from coercion and manipulation by others, he must be independent." Joseph Raz, The Morality of Freedom 376 (1986)

This is not to suggest an absolute account of autonomy. "[T]he autonomous person is a (part) author of his own life. The ideal of personal autonomy is the vision of people controlling, to some degree, their own destiny, fashioning it through successive decisions throughout their lives." *Id* at 369. In the section dealing with GRP_2, I highlight how algorithmic grouping violates an individual's autonomy by manipulation and in some cases active discrimination.

33 Hogg, *supra* note 14, at 6 (describing how social groups foster the creation of a shared identity for their members).

34 *See* OSCAR GANDY, THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION. CRITICAL STUDIES IN COMMUNICATION AND IN THE CULTURAL INDUSTRIES 20 (1993), https://eric.ed.gov/?id=ED377817. As early as 1993, Gandy had highlighted the perils of panoptic sort, a discriminatory process that sorts individuals based on their estimated value. *Id.*

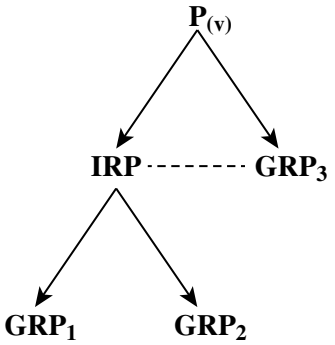
35 ("Behavioral targeting aims to group users into segments of similar behaviors and deliver different ads to different groups of users.") *See* Jun Yan, Ning Liu, Gang Wang, Wen Zhang, Yun Jiang, & Zheng Chen, *How Much Can Behavioral Targeting Help Online Advertising?*, PROC. OF THE 18TH CONF. ON THE WORLD WIDE WEB 263 (2009) (providing an empirical study on the click-through log of advertisements collected from a commercial search engine).

36 *See* C. Thi Nguyen, *Echo Chambers and Epistemic Bubbles*, 17 EPISTEME 141, 142 (2020) (". . . an epistemic bubble is a social epistemic structure in which some relevant voices have been excluded through omission.").

37 *See id.* ("An echo chamber . . . is a social epistemic structure in which other relevant voices have been actively discredited.").

formation of an individual's social identity. GRP_1 seeks to safeguard an individual's social identity and socially embedded, autonomous self against this intrusion.

In addition to protecting their membership in social groups, an individual also has an interest against algorithmic grouping, which is steeped in their right to informational self-determination.[38] Algorithmically grouping an individual on the basis of their online activity is a violation of their autonomy.[39] I recognize and seek to protect this interest through GRP_2, the right against algorithmic grouping. Lastly, I acknowledge that there are scenarios where certain organized groups have an independent right to privacy, which is not reducible to an individual right to privacy. I seek to protect this group interest in privacy through GRP_3.[40] The protection of this group interest in privacy can offer additional protection to individual privacy. The theoretical model is depicted below:



I develop a Razian formulation of GRP to state that Big Data Analytics's constant surveillance and monetization of human existence is an infringement of individual autonomy.[41] I highlight that the violation of

---

[38] *See* J. C. Buitelaar, *Post-mortem Privacy and Informational Self-Determination*, 19 ETHICS INFO. TECH. 129, 137 (2017) (exploring whether right to informational self-determination has validity in postmortem context.). Buitelaar states that informational self-determination is the individual's "capacity to determine without coercion which information about [them] and will be available and accessible." *Id.*

[39] *See* Kammourieh et al., *supra* note 7, at 43 (defining privacy as a facet of human dignity and discussing how Big Data groups individuals without their knowledge). I further share the concerns raised by Kammourieh et al. that algorithmic grouping is a violation of the right to privacy which is based in human dignity.

[40] *Cf.* Bart van der Sloot, *Do Groups Have a Right to Protect Their Group Interest in Privacy and Should They? Peeling the Onion of Rights and Interests Protected Under Article 8 ECHR*, *in* GROUP PRIVACY-NEW CHALLENGES OF DATA TECHNOLOGIES 197, 213–14 (Linnet Taylor, Luciano Floridi, & Bart van der Sloot eds., 2017) (stating "If it is true that these relationships are built and dependent on the protection of privacy, the violation of privacy is something more than an aggregated interests of several individuals. It is a constitutive element of the group as such.").

[41] *See* Kirstie Ball & Frank Webster, *The Intensification of Surveillance*, in THE INTENSIFICATION OF SURVEILLANCE: CRIME, TERRORISM AND WARFARE IN THE INFORMATION ERA 1, 1

GRP subjects an individual to behavioral targeting (including hyper-targeted political advertising) and distorts their *weltanschauung*, or worldview.[42] As regards the Covid-19 Apps, I assert that the pandemic's extraordinary circumstances do not provide an everlasting justification for reducing an individual's identity to a potential disease carrier. I argue that the ambivalence regarding the existence of surveillance surrounding an individual's social identity can leave them in a perpetual state of simulated surveillance (simveillance).[43]

In conclusion, I highlight that our privacy is not only interdependent in nature, but is existentially, cumulatively interlinked. It increases in force with each successive protection. I challenge the privacy versus access tradeoff and highlight the global regulatory trends in favor of privacy. I further argue that it is in Big Tech corporations' long-term interest to respect privacy. I state that the privacy challenge posed by Covid-19 Apps has helped us realize that while limited exceptions to privacy maybe carved out in grave emergencies, there is no moral justification for round- the- clock surveillance of an individual's existence by Big Data Analytics. Similarly, the threat to privacy posed by Big Data Analytics has helped us realize that privacy has been wrongly focusing on the distinguishing aspects of the individual. It is our similarities that are truly worth protecting. In order to protect these similarities, I formu-

---

(Ball & Webster eds., 2003). As per Ball & Webster, "Surveillance involves the observation, recording and categorization of information about people, processes and institutions. It calls for the collection of information, its storage, examination and—as a rule—its transmission." *Id.* As per Zuboff, "Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data." SHOSHANNA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 8 (2019); *see also* Jonathan Cinnamon, *Social Injustice in Surveillance Capitalism*, 15 SURVEILLANCE & SOC'Y 609, 611–12 (". . . personal data accumulation by surveillance capitalists is not only an economic injustice of maldistribution, it is also the key mechanism by which two further, more opaque forms of injustice are made possible. The initial injustice of personal data maldistribution can lead to sociocultural misrecognition, which occurs when personal data are subject to algorithmic processing and classification, as well as political misrepresentation, which renders people voiceless to challenge any misuse of their personal data.").

42 Merriam Webster defines *Weltanschauung* as "a comprehensive conception or apprehension of the world especially from a specific standpoint." *Weltanschauung*, MERRIAM-WEBSTER.COM DICTIONARY, https://www.merriam-webster.com/dictionary/Weltanschauun. *Weltanschauung* refers to "the worldview of an individual or group." *Weltanschauung*, LEXICO, https://www.lexico.com/en/definition/weltanschauung.

43 The portmanteau "simveillance" arises out of "simulation" and "surveillance." WILLIAM BOGARD, THE SIMULATION OF SURVEILLANCE: HYPERCONTROL IN TELEMATIC SOCIETIES 4 (Cambridge Univ. Press 1996). (". . . technologies of simulation are forms on *hypersurveillant control*, where the prefix "hyper" implies not simply an intensification of surveillance, but the effort to push surveillance technologies to their absolute limit. That limit is an imaginary line beyond which control operates, so to speak, in 'advance' of itself and where surveillance—a technology of exposure and recording—evolves into a technology of *pre*-exposure and *pre*-recording, a technical operation in which all control functions are reduced to modulations of preset codes."). *Id.*

late the concept of mutual or companion privacy, which counter-intuitively states that in the age of Big Data Analytics we have more privacy together rather than individually.

In order to systematically develop the theoretical framework, this Article has been divided into eleven parts. Part I traces the evolution of privacy from an individual right to a group right. Part II analyzes the threat to privacy in the age of Big Data Analytics. Part III examines the impact of Covid-19 Apps on individual identity and autonomy. Part IV explores privacy's role in identity formation. Part V highlights the importance of privacy in protecting the socially embedded, autonomous self. Part VI provides a primer to the triumvirate formulation of the group right to privacy. Part VII develops GRP_1, which seeks to protect an individual's interest in their socially embedded, autonomous self and social identity arising out of participation in social groups. Part VIII emphasizes an individual's right to informational self-determination and against algorithmic grouping in the form of GRP_2. Part IX highlights instances where an organized group may have an entitlement to privacy in its own right as GRP_3. Part X highlights the harms suffered because of violation of the GRP formulation. Finally, Part XI prescribes the way forward in the form of mutual or companion privacy.

I. THE EVOLUTION OF PRIVACY: FROM INDIVIDUAL TO GROUP

As noted in the introduction, the right to privacy began its jurisprudential journey as the individual's "right to be let alone."[44] Over the course of a century, even as the focus of privacy has shifted from physical intrusion to information privacy,[45] the locus of privacy continues to be the individual.[46] However, overemphasis on individual privacy has led to the neglect of privacy's social aspects, the weakening of privacy in political practice, and the failure of privacy regulation to keep pace with technological developments.

---

44 Warren & Brandeis, *supra* note 2, at 193.

45 *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 2 (5th ed. 2014). As per Solove & Schwartz, "Information privacy concerns the collection, use, and disclosure of personal information. Information privacy is often contrasted with 'decisional privacy,' which concerns the freedom to make decisions about one's body and family." *Id.*

46 *See* Balachander Krishnamurthy & Craig E. Wills, *On the Leakage of Personally Identifiable Information via Online Social Networks*, *in* PROCEEDINGS OF THE 2ND ACM WORKSHOP ON ONLINE SOCIAL NETWORKS 7 (Jon Crowcroft ed., 2009) (exploring the possibility of third party's linking personally identifiable information, which is leaked via social networks with other user actions). The individual's information privacy is presently protected through the regulatory device called "Personally Identifiable Information." As per Balachander & Wills, "Personally identifiable information is information, which can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linkable to a specific individual." *Id.*

As regards social aspects, privacy is not just an individual right but also a social good.[47] Further, the traditional view of privacy, which is focused on protecting individual interests, has provided a weak basis for protecting privacy in the political realm.[48] Mokrosinska and Roessler note, "[w]hen individual privacy conflicts with broader social interests such as law enforcement, public security, or the implementation of social justice, protecting individuals' interests seems to be a luxury that society can ill afford."[49] As regards the technological challenge, with the advent of big data and analytical tools for profiling, it is possible to violate an individual's privacy even without identifying them.[50] In all fairness, when Warren and Brandeis expounded the right to privacy, it would have been axiomatic to conceptualize privacy solely from an individual perspective.[51] In the absence of Information and Communication Technologies (ICTs), it would have made eminent sense to seek privacy *from* a group rather than *in* a group. The realization of the social, political, and technical limitations of the individual right to privacy is the genesis of the group right to privacy.

Floridi offers the justification for group privacy in the age of Big Data Analytics by stating, "[s]ometimes the only way to protect the individual is to protect the group to which the individual belongs. Preferably before any disaster happens."[52] In their work on group privacy, Taylor, Floridi, and van der Sloot provide the following cogent justification for group privacy in present day and age: ". . . in an era of big data where analytics are being developed to operate at as broad a scale as possible,

---

47 *See* Debbie V.S. Kasper, *Privacy as a Social Good*, 28 SOC. THOUGHT & RSCH. 165, 165 (2007). See also: Regan *supra* note 16 at 50. Valerie Steeves, Reclaiming the social value of privacy, in LESSONS FROM THE IDENTITY TRAIL 191, 193-194 (Ian Kerr et al ed. 2009). (highlighting the social value of privacy.)

48 *See* Annabelle Lever, *Privacy Rights and Democracy: A Contradiction in Terms?*, 5 CONTEMP. POL. THEORY 142, 142 (2006) (detailing information about privacy's role in enabling democratic expression and communication).

49 Dorota Mokrosinska & Beate Roessler, *Introduction*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 3 (Roessler & Mokrosinska eds., 2015) (reflecting on the social dimensions of privacy).

50 Linnet Taylor, *Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 13, 14 (Linnet Taylor, Luciano Floridi, & Bart van der Sloot eds., 2017) (arguing that group privacy is a necessary element of a global perspective on privacy); *see also* Alessandro Mantelero, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, *in* GROUP PRIVACY—NEW CHALLENGES OF DATA TECHNOLOGIES 139, 145 (Linnet Taylor, Luciano Floridi, & Bart van der Sloot eds., 2017) (investigating the opportunity to consider informational privacy and data protection as collective rights in the age of big data analytics).

51 *See* Warren & Brandeis, *supra* note 2, at 193, 196–97.

52 Luciano Floridi, *Open Data, Data Protection, and Group Privacy*, 27 PHIL. & TECH. 1, 3 (2014) (exploring the debate between open data and data protection through the prism of group privacy).

the individual is often incidental to the analysis. Instead, data analytical technologies are directed at the group level."[53]

Floridi claims that groups are neither invented nor discovered, but designed by the level of abstraction (LoA) at which a specific analysis of a social system is developed.[54] As per this claim, the logical order is purpose (why individuals are being grouped in this way) followed by LoA (how individuals are being grouped in this way) and then result (the obtained group).[55] Floridi states that the very same practices that determine the grouping of people also delineate the resulting groups as potential holders of a privacy right.[56] Building upon Floridi's work, Loi and Christen identify two forms of group rights to privacy: the first concerning the confidential information shared with the group members, and the second concerning the inferences that one can draw about the group members because of shared features.[57] Mittelstadt has argued that algorithmically-assembled groups or ad hoc groups "should be formally recognized as moral patients in data protection law and privacy theory."[58]

Despite these attempts at expanding the scope of privacy, recent perspectives on privacy recognize that group privacy is falling short in face of emerging data analytic techniques.[59] Further, there is a lack of an overarching theoretical framework for the group right to privacy.[60] The history of human rights demonstrates the necessity of such a framework. Human rights scholars identify the lack of philosophical justifications at the time of Human Rights Declaration as a major reason for the vulnerability of human rights.[61] Sen, while noting the impatience of human rights activists with theoretical criticisms and conceptual doubts, states that "[i]t is not hard to understand their unwillingness to spend time trying to provide conceptual justification, given the great urgency to re-

---

53 Taylor, Floridi, & van der Sloot, *supra* note 8, at 2.

54 Floridi, *supra* note 19, at 83.

55 *Id.* at 88.

56 *Id.* at 89.

57 Michele Loi & Markus Christen, *Two concepts of Group Privacy*, 33 PHIL. & TECH. 207, 207 (2020) (discussing two concepts of group privacy-one involving confidential information shared between the members of a group and second dealing with inferences that can be made regarding the members of a group).

58 Brent Mittelstadt, *From Individual to Group Privacy in Big Data Analytics*, 30 PHIL. & TECH. 475, 492 (2017).

59 *See* Taylor, Floridi, & van der Sloot, *supra* note 8, at 2.

60 *See id.* at 3. The authors, while describing the various scholarship approaches to defining group privacy in their work, states that their approaches are functional and iterative rather than stable and unanimous. *Id.*

61 Johannes Morsink, *World War Two and the Universal Declaration*, 15 HUM. RTS. Q. 357, 397 (1993) ("It seems, therefore, that the war, which prompted the writing of a Declaration with a set of universal and absolute values, did not provide a philosophy with which to defend that set.").

spond to terrible deprivations around the world . . . However, the conceptual doubts must also be satisfactorily addressed, if the idea of human rights is to command reasoned loyalty and to establish a secure intellectual standing."[62] My conceptualization of a theory of group privacy is driven by a similar motivation to provide philosophical justifications for an expansion of privacy in the age of Big Data Analytics. Before I elaborate my theoretical framework, it is important to understand the threat Big Data Analytics pose to privacy.

II. PRIVACY IN THE AGE OF BIG DATA

Big Data can be functionally understood as "the process of applying serious computing power—the latest in machine learning and artificial intelligence—to seriously massive and often highly complex sets of information."[63] Why Big Data is a threat to privacy becomes intuitively clear with the help of a widely cited definition: "Big Data is the Information asset characterized by such a High Volume, Velocity and Variety to require specific Technology and Analytical Methods for its transformation into Value."[64] The use of massive computational power to transform human experience into a data set of value is a direct threat to individual autonomy and consequently a challenge for privacy. As a report commissioned by the White House on Big Data notes, "[a]nother concern is that big data technology could assign people to ideologically or culturally segregated enclaves known as 'filter bubbles' that effectively prevent them from encountering information that challenges their biases or assumptions."[65]

Stephens-Davidowitz enumerates four powers of Big Data that can be distilled as the Big Data's ability to use new forms of immensely honest data sets to zoom in on small subsets of the population and con-

---

62 Amartya Sen, *Elements of a Theory of Human Rights*, 32 PHIL. & PUB. AFFS. 315, 317 (2004) (presenting the elements of a theory of human rights).

63 Jonathan Stuart Ward & Adam Baker, *Undefined By Data: A Survey of Big Data Definitions*, ARXIV (2013), https://arxiv.org/pdf/1309.5821.pdf (collating the various definitions of Big Data.); *see also* Microsoft, *The Big Bang: How the Big Data Explosion Is Changing the World*, MICROSOFT UK ENTERPRISE INSIGHTS BLOG (April 15, 2013), https://blogs.msdn.microsoft.com/microsoftenterpriseinsight/2013/04/15/the-big-bang-how-the-big-data-explosion-is-changing-the-world/.

64 Andrea De Mauro, Marco Greco & Michele Grimaldi., *A Formal Definition of Big Data Based on its Essential Features*, 65 LIBR. REV. 122, 122 (2016) (identifying and describing the most prominent research areas connected with "Big Data" and proposing a thorough definition of the term).

65 EXEC. OFFICE OF THE PRESIDENT, BIG DATA, SEIZING OPPORTUNITIES, PRESERVING VALUES (2014); *see also* Cynthia Dwork & Deirdre K. Mulligan, *It's Not Privacy, and It's Not Fair*, 66 STAN. L. REV. ONLINE 35, 36 (2013) (discussing the insufficiency of privacy controls against the classification power of big data).

duct a highly causal analysis.[66] I will address specific examples of how Big Data Analytics infringe on privacy and undermine individual autonomy later in the Article. I also analyze some of the shortcomings of the existing privacy framework which result in violation of individual identity and autonomy:

A. Lacunae in the Existing Privacy Framework:

1. Shifting focus: Schonberger and Cukier highlight that with the advent of Big Data Analytics, the value of information no longer resides solely in its primary purpose for which it was collected, but in its secondary uses.[67] Kammoureih and others state that the traditional right to privacy focuses solely on information collection rather than analysis and is thus no longer a fully effective instrument of control.[68]
2. Onus on the individual: The existing model of collecting an individual's data on the basis of "notice and consent" is deeply flawed. It has now become a cliché to state that nobody reads a website's privacy policy, but it is still important to state that even the best of trained experts would be hard-pressed to interpret the unilateral and ambiguous privacy policies.[69] Hence, there is no informed consent.[70]
3. Contextual integrity: Nissenbaum advocates a contextual approach to privacy online, emphasizing the importance of contextual integrity as personal information moves across heterogeneous online contexts.[71] She states that "[c]ontextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it."[72] While this does

---

66 SETH STEPHENS-DAVIDOWITZ, EVERYBODY LIES: BIG DATA, NEW DATA AND WHAT THE INTERNET CAN TELL US ABOUT WHO WE REALLY ARE 53–54 (2017).

67 VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK AND THINK 103 (2013).

68 Kammourieh et al., *supra* note 7, at 46.

69 Masooda Bashir, April D. Lambert, Carol Hayes, & Jay P. Kesan, *Online Privacy and Informed Consent: The Dilemma of Information Asymmetry*, 52 PROC. ASS'N FOR INFO. SCI. & TECH. 1, 2 (2016) (discussing the problem of information asymmetry in privacy and consent). *See also* Marcus Moretti & Michael Naughton, *Why Policies are so Inscrutable*, THE ATLANTIC (Sep. 5, 2014), https://www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615/.

70 Masooda Bashir, April D. Lambert, Carol Hayes, & Jay P. Kesan, *supra* note 69.

71 Helen Nissenbaum, *A Contextual Approach to Privacy Online*, DAEDALUS 32, 41 (2011) (articulating context-specific substantive norms that constrain what information websites can collect, with whom and under what conditions it can be shared).

72 Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 119 (2004) (explaining why some of the prominent theoretical approaches to privacy, which were

offer a modicum of privacy, it assumes that the aggregator or gatherer of information is aware of all the uses of the information collected under the ambit of the privacy policy, which very often is not the case.[73] The usage of broad-based terms, such as "commercial purposes" in the privacy policy, further undermines the contextual integrity of data.[74]

4. Restricted access and anonymity: Wu, Zhu, Wu, and Ding state that two common approaches to protect privacy are to:

   a) "[R]estrict access to the data, such as adding certification or access control to the data entries, so sensitive information is accessible by a limited group of users only, and

   b) [A]nonymize data fields such that sensitive information cannot be pinpointed to an individual record."[75]

   The restricted access approach is not entirely effective because, as stated earlier, identification is not necessary to influence the individual.[76] Further, it is virtually impossible to completely anonymize data.[77]

5. Differential privacy: Differential privacy focuses on disclosing properties of a database while protecting individual information. As per the Harvard University Privacy Tool Project, "an algorithm is said to be differentially private if by looking at the

---

developed over time to meet traditional privacy challenges, yield unsatisfactory conclusions in the case of public surveillance).

73 "A major problem created by the widespread adoption of computer and telecommunications technology to personal-data record keeping is the inability to anticipate and control future use of information." PRIVACY PROTECTION STUDY COMMISSION, TECHNOLOGY AND PRIVACY: APPENDIX 5 TO THE REPORT OF THE PRIVACY PROTECTION STUDY COMMISSION 26 (1977). *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, GEO. WASH. L. FAC. PUBL'NS 1814, 1846 (2011) (noting the problems of defining PII).

74 *See generally* Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html?mtrref=www.google.com&assetTypeREGIWALL. *See generally* Moretti & Naughton, *supra* note 69.

75 Xindong Wu, Xingquan Zhu, Gong-Qing Wu, & Wei Ding, *Data Mining with Big Data*, 26 IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENG'G 97, 100 (2014) (analyzing the challenging issues in the data-driven model and also in the Big Data revolution); *see also* Graham Cormode & Divesh Srivastava, *Anonymized Data: Generation, Models, Usage*, IEEE XPLORE 1211, 1211 (2010), https://ieeexplore.ieee.org/document/5447721 (describing how the body of "work in query evaluation over uncertain databases can hence be used for answering ad hoc queries over anonymized data" in a principled manner).

76 Barocas & Nissenbaum, *supra* note 6, at 45.

77 A recent study published in Nature Communications states that even heavily sampled anonymized datasets are unlikely to satisfy the modern standards for anonymization the EU General Data Protection Regulation (GDPR) set forth. For instance, it is possible to re-identify 99.98% of Americans in any dataset using 15 demographic attributes. Luc Rocher, Julien M. Hendrickx, & Yves-Alexandre de Montjoye, *Estimating the Success of Re-identifications In Incomplete Datasets Using Generative Models*, 10 NATURE COMM. 1, 5 (2019).

> output, one cannot tell whether any individual's data was included in the original dataset or not."[78] While exploring database privacy Dwork notes, Dalenius desideratum for statistical databases articulated in 1977, "[n]othing about an individual should be learnable from the database that cannot be learned without access to the database."[79] After stating that Dalenius' desideratum is impossible to achieve, Dwork argues that differential privacy provides an alternative to anonymization of data by adding random noise to make databases resilient to adaptive attacks that use auxiliary information.[80] However, as Arpita Ghosh and Robert Kleinberg highlight,
>
> [D]ifferential privacy focuses on the privacy loss to an individual by [their] contribution to a dataset, and therefore—by design—does not capture all of the privacy losses from inferences that could be made about one person's data due to its correlations with *other* data in networked contexts.[81]

It is this lacuna that Big Data Analytics exploits.

The aforesaid discussion clarifies that the various downstream approaches to correct individual malaise arising out of data practices have not succeeded. In order to thwart Big Data Analytics's assault on individual autonomy and identity, it is important to justify a strong moral interest in comprehensive protection of the group affiliations that constitute an individual's identity and autonomy. While discussing Bank of England's monetary policy, Graeber wrote: "[B]ack in the 1930s, Henry Ford is supposed to have remarked that it was a good thing that most Americans didn't know how banking really works, because if they did, 'there'd be a revolution before tomorrow morning.'"[82] Something similar can be said about Big Data Analytics. As Stephens-Davidowitz states,

---

78 *Differential Privacy*, HARV. UNIV. PRIV. TOOLS PROJECT, https://privacytools.seas.harvard.edu/differential-privacy (last visited Oct. 7, 2020).

79 Tore Dalenius, *Towards a Methodology for Statistical Disclosure Control*, 15 STATISTIK TIDSKRIFT 429, 433 (1977) (articulating a desideratum for statistical databases); *see also* Cynthia Dwork, *Differential Privacy: A Survey of Results*, RESEARCHGATE 1, 2–3 (Apr., 2008), https://www.researchgate.net/publication/220908334_A_Practical_Parameterized_Algorithm_for_the_Individual_Haplotyping_Problem_MLF (discussing the increased risk to one's privacy incurred by participating in a database); *see also* Cynthia Dwork, *Differential Privacy*, in AUTOMATA, LANGRAGES & PROGRAMMING ICALP LECTURE NOTES IN COMPUTER SCIENCE 1 (Bugliesi et. al eds., 2006).

80 *See* Dwork, *supra* note 79 at 9; *see also* Aaruran Elamurugaiyan, *A Brief Introduction to Differential Privacy*, MEDIUM: GEORGIAN IMPACT BLOG (Aug. 31, 2018), https://medium.com/georgian-impact-blog/a-brief-introduction-to-differential-privacy-eacf8722283b.

81 Arpita Ghosh & Robert Kleinberg, *Inferential Privacy Guarantees for Differentially Private Mechanisms*, ARXIV (May 23, 2017), https://arxiv.org/pdf/1603.01508.pdf (asking how differential privacy guarantees translate to guarantees on inferential privacy in networked contexts) (emphasis original).

82 David Graeber, *The Truth Is Out: Money Is Just An IOU, And the Banks Are Rolling In It*, GUARDIAN (Mar. 18, 2014), https://www.theguardian.com/commentisfree/2014/mar/18/

"[t]his is the ethical question: Do corporations have the right to judge our fitness for their services based on abstract but statistically predictive criteria not directly related to those services?"[83] If more of us understood how Big Data Analytics undermine our autonomy, identity, and privacy, there would be a greater uproar resulting in better regulation. I enumerate my vision of this better regulation in the ensuing parts. Before that, I highlight the novel threat posed by Covid-19 Apps to individual privacy. I will then develop a model to jointly address the privacy concerns raised by both Big Data Analytics and Covid-19 Apps.

III. PANDEMIC AND PRIVACY

In the aftermath of the Covid-19 pandemic, many countries launched health surveillance apps as part of the effort to contain the virus's spread through contact tracing.[84] Experts disagree on the feasibility and desirability of such apps.[85] While proponents of these apps point to their potential efficacy, privacy scholars have voiced their concerns regarding their potential overreach.[86] It is also worth noting that while

---

truth-money-iou-bank-of-england-austerity (discussing Bank of England's paper "Money creation in the Modern Economy").

83 STEPHENS-DAVIDOWITZ, *supra* note 66, at 261.

84 Paul Schwartz, *Protecting Privacy On COVID-19 Surveillance Apps*, IAAP (May 8, 2020), https://iapp.org/news/a/protecting-privacy-on-covid-surveillance-apps/.

85 Luca Ferretti et al., *Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control With Digital Contact Tracing*, 368 SCIENCE 619, 620 (May 8, 2020) ("A contact-tracing app that builds a memory of proximity contacts and immediately notifies contacts of positive cases can achieve epidemic control if used by enough people."). A report by the Pathogen Dynamics Group, Big Data Institute, Nuffield Department of Medicine, and University of Oxford found "that the epidemic can be suppressed with 80% of all smartphone users using the app, or 56% of the population overall." ROBERT HINCH ET AL., EFFECTIVE CONFIGURATIONS OF A DIGITAL CONTACT TRACING APP: A REPORT TO NHSX 3 (Apr. 16, 2020), https://cdn.theconversation.com/static_files/files/1009/Report_-_Effective_App_Configurations.pdf?1587531217. On how to make mobile phone data work against the virus, see Nuria Oliver et al., *Mobile Phone Data For Informing Public Health Actions Across The COVID-19 Pandemic Life Cycle*, 6 SCI. ADVANCES 1, 1 (June 5, 2020). On the other hand, Piotr Sapiezynski et al. challenged the assumptions underlying Contact-Tracing Apps and warned "about the potential consequences of over-extending the existing state and corporate surveillance powers." Piotr Sapiezynski, Johanna Pruessing & Vedran Sekara, *The Fallibility of Contact-Tracing Apps*, ARXIV (May 27, 2020), https://arxiv.org/pdf/2005.11297.pdf. Federica Lucivero et al. argue "that rather than technological fixes to the current emergency these apps should be introduced in society as societal experimental trials whose effectiveness and consequences need to be closely and independently monitored the same level of precaution and safeguards that social experimentation require." Federica Lucivero, Nina Hallowell, Stephanie Johnson, Barbara Prainsack, Gabrielle Samuel & Tamar Sharon, *Covid-19 and Contact Tracing Apps: Technological Fix or Social Experiment?*, SSRN (Apr. 10, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3590788&download=yes.

86 Neema Singh Guliani, *ACLU Government Safeguards for Tech-Assisted Contact Tracing*, ACLU (May 18, 2020), https://www.aclu.org/other/aclu-white-paper-government-safeguards-tech-assisted-contact-tracing.

some countries have steadfastly adopted this techno-legal solution, others have been far more circumspect, with Norway even abandoning the project on account of privacy concerns.[87]

Parker, Fraser, Abeler-Dörner, and Bonsall summarize the ethical dilemmas surrounding the Covid-19 Apps as

> The scale of the suffering caused by the COVID-19 pandemic means that if a case can be made that some degree of privacy infringement will save significant numbers of lives and reduce suffering, the intervention may be justified. Any such justification will depend on a clear case being made that the privacy infringement is either necessary or that it is significantly more effective than the alternatives. One aspect of a convincing attempt at justification might be the claim that the privacy infringement is less intrusive than blanket population level lockdowns for everyone. It would, however, also require a convincing case to be made that (i) any privacy impact would be minimized, (ii) that high standards of data security, protection and oversight would be in place, (iii) that there would be transparency about proposed and actual data uses, and (iv) that these would be complemented by other protections, for example, around non-discrimination.[88]

The real challenge lies in converting this moral position into an applicable legal principle. Barring a few studies on ethical implications, the existing scholarship on Covid-19 Apps has largely focused on technical solutions to safeguard the individual's privacy.[89] We have been focusing on what data is being collected, its anonymization, duration and place of storage, and access to the said data.[90] In other words, we have been focusing on identification and mimicking the existing safeguards that we deploy against Big Data Analytics. These are important safeguards, but in the absence of an operational legal tenet, this piecemeal approach is

---

87 Agence France-Presse in Oslo, *Norway Suspends Virus-Tracing App Due To Privacy Concerns*, GUARDIAN (June 15, 2020), https://www.theguardian.com/world/2020/jun/15/norway-suspends-virus-tracing-app-due-to-privacy-concerns.

88 Parker et al., *supra* note 4, at 428 (discussing ethical implications of the use of mobile phone apps in the control of the COVID-19 pandemic).

89 Justin Chan et al., *PACT: Privacy-Sensitive Protocols and Mechanisms for Mobile Contact Tracing*, ARXIV (May 7, 2020), https://arxiv.org/pdf/2004.03544.pdf (suggesting functionalities for harnessing computing technologies to minimize "mortality associated with the spread of COVID-19, while protecting the civil liberties of individuals."); Qiang Tang, *Privacy-Preserving Contact Tracing: current solutions and open questions*, ARXIV (Apr. 25, 2020), https://arxiv.org/pdf/2004.06818.pdf (examining "existing privacy-aware contact tracing solutions and analys[ing] their (dis)advantages").

90 Chan et al., *supra* note 89, at 12.

less likely to succeed. In order to balance privacy interests with larger public health concerns, instead of focusing on identification, we need to focus on identity construction.

Towards this end, it is critical to note that there are important differences between the functioning of Big Data Analytics and the Covid-19 Apps. Big Data Analytics control our access to the physical realm through the virtual.[91] On the other hand, Covid-19 Apps exercise direct control over our participation in the physical realm.[92] In ordinary circumstances, an individual participates in the social sphere through the various roles that they perform, such as a parent or a professor. An individual's control over determination of their social identity is a fundamental aspect of an their autonomy, which is protected through privacy. However, during the extraordinary course of the pandemic, an individual's participation in the social sphere becomes contingent on their status as a potential disease carrier as determined by the Covid-19 Apps. One could argue that the diminished individual control over social identity is not the result of Covid-19 Apps but of the pandemic. However, such a claim would not be entirely correct. While the extraordinary circumstances of pandemic certainly play a part in diminishing individual autonomy, it is the technical surveillance solutions, such as the Covid-19 Apps, that make the pandemic relevant from privacy studies perspective. Covid-19 Apps are technological embodiments of Foucault's "medical gaze," the accumulation of medical knowledge through the "medical separation between a patient's body and his identity."[93] Unlike Big Data Analytics, which deploys opaque strategies to diminish individual autonomy, Covid-19 Apps exercise visible direct control.[94] While most countries have made the installation of these Apps voluntary, privacy scholars

---

91 *See* Alessandro Mantelero, *Social Control, Transparency and Participation in the Big Data World*, JOURNAL OF INTERNET LAW 23, 27 (2014). ("Governments and big companies are increasing their control over information. This concentration is reducing the transparent and democratic use of information in our societies, facilitating social control, and producing an asymmetric distribution of knowledge in society"). *See also* EXEC. OFFICE OF THE PRESIDENT, *supra* note 65, at 7–8 (explaining that Big Data Analytics leads to "discrimination in pricing, services, and opportunities" and can "effectively prevent [individuals] from encountering information that challenges their biases or assumptions.").

92 In China, individuals must scan a Covid-19 App based QR code before entering public places and can be denied entry depending on their "health score." *See* Anna Gamvros & Libby Ryan, *How Contact Tracing Apps in Asia Are Being Used To Fight COVID-19 – Is the Reward Worth the Risk?*, DATA PROT. REP. (Apr. 24, 2020), https://www.dataprotectionreport.com/2020/04/how-contact-tracing-apps-in-asia-are-being-used-to-fight-covid-19-is-the-reward-worth-the-risk/.

93 Black Hawk Hancock, *Michel Foucault and the Problematics of Power: Theorizing DTCA and Medicalized Subjectivity*, 43 J. MED. & PHIL. 439, 443 (2018) (exploring Foucault's different notions of power).

94 *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 65, at 10 ("Some of the most profound challenges revealed during this review concern how big data analytics may lead to disparate inequitable treatment, particularly of disadvantaged groups, or create such an opaque

have decried this consent as illusory.[95] This illusory consent and the resultant compulsory installation of these Apps places a limitation on an individual's right to informational self-determination.

A surveillance app that reduces an individual's identity to a potential disease carrier and acts as a gatekeeper to their participation in the social sphere faces an enormous moral challenge. The right to "freely pursue the development and fulfillment" of one's identity is a fundamental human right.[96] Any app seeking to temporarily suspend that right needs to meet a much higher benchmark than the anonymity guaranteed in privacy regulation. It must be in conformity with the morality of freedom.[97] This higher benchmark that I seek cannot come by restricting our

---

decision-making environment that individual autonomy is lost in an impenetrable set of algorithms."); Gamvros & Ryan, *supra* note 92.

95 As per Schwartz, "the critical issue is how the government and private sector will restrict access to spaces and opportunities based on whether or not one 'consents' to the use of an app or other monitoring device." Paul Schwartz, *Illusions of Consent and COVID-19-Tracking Apps*, IAPP (May 19, 2020) https://iapp.org/news/a/illusions-of-consent-and-covid-tracking-apps/.

96 COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, GUIDE ON ARTICLE 8 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS, 55 (2020), https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

97 *See* JOSEPH RAZ, THE MORALITY OF FREEDOM 267 (1988) (stating "[m]orality is . . . concerned with the advancement of the well-being of individuals."). For Raz, Morality is not based in rights, but its foundation lies in duties, goals, virtues etc. *Id* at 193. The relationship between freedom and morality can be understood from the perspective, "[s]ignificantly autonomous persons . . . who can shape their life and determine its course . . . are part creators of their own moral world." *Id* at 154. Importantly for Raz, personal autonomy is incompatible with moral individualism but linked to collective goods. *Id* at 206–07, 247. Raz's co-relation of personal autonomy with collective goods plays an important role in developing my account of privacy as a social value in subsequent parts. *See also* Donald H. Regan, *Authority and Value: Reflections on Raz's* Morality of Freedom, 62 S. CAL. L. REV. 995, 1000 (1989). In *Morality of Freedom*, Raz aims to develop a liberal foundation for a political morality. Donald Regan has summarized Raz's views on autonomy as,

> (1) genuine autonomy requires the existence of a wide range of social practices which define activities and relationships (such as being a doctor, being a concert violinist, marriage, friendship, and so on); (2) the existence of any such social practice is a collective good; (3) individuals do not have rights to the existence of such collective goods; therefore, (4) individuals do not have rights to the conditions of autonomy.

See Roger A. Shiner, *Reviewed Work(s): The Morality of Freedom by Joseph Raz*, 63 PHIL. 119, 119 (1988). Philosophers world over have expounded upon the virtues of freedom and explored its relationship with morality. J. Krishnamurti writes,

> [F]reedom is one of the most important factors in life. . .So when we talk of freedom we are talking of the fundamental issue. It is not a freedom from something, but the quality of a mind and heart that are free, and in which direction does not exist. Freedom from something is only a modified continuity of what has been, and therefore it is not freedom. When there is direction, and therefore choice, freedom cannot exist; for direction is division and hence choice and conflict.

Without responsibility there is no Freedom, J. KRISHNAMURTI: Teachings, https://jkrishnamurti.org/content/chapter-66-without-responsibility-there-no-freedom.

For Amartya Sen, the expansion of freedom is the primary end as well as the principal means of development. *See* AMARTYA SEN, DEVELOPMENT AS FREEDOM xii (1999). In the

focus to the identification of the individual. We need to analyze the role privacy plays in the formation of an individual's identity. Similarly, if we have to design an effective theoretical framework to thwart Big Data Analytics's impingement of individual identity and autonomy, we must address the question of why individuals are sharing their data in the first place. In the next section, I explore the hypothesis that individuals share their data online as part of the development of their social identity. Privacy plays a pivotal role in guarding the formulation of this social identity from the intrusion of Big Data Analytics. This hypothesis shifts the paradigm of privacy studies from identification to identity formation and forms the basis of group right to privacy.

IV. PRIVACY AND IDENTITY

Privacy scholars disagree on many aspects of privacy, including its definition.[98] However, there is a greater consensus that privacy plays an important role in protecting an individual's identity and autonomy.[99] My expansive account of privacy is built on the edifice of this consensus. I seek an account of privacy that can meaningfully protect individual identity and autonomy against Big Data Analytics and Covid-19 Apps. Any such exercise must begin with an account of individual identity and autonomy that one seeks to protect through privacy. In the ensuing paragraphs, I argue that for the purposes of privacy protection, an individual's identity is not limited to their personal identity, but also extends to their social identity. Further, the autonomous self that is sought to be protected through privacy is not a secluded liberal self, but the socially embedded autonomous self.

A. The Concept of Self

Mercadal states "[t]he nature of the self—what it is and how it works—has been a human preoccupation since ancient times."[100] As per Rodriguez, "[a] person's self-concept derives from two principal sources: personal identity and social identity. Personal identity includes one's individual traits, achievements, and qualities. Social identity includes the group affiliations that are recognized as being part of the self, such as one's image of oneself as a Protestant, a blue-collar worker, or a con-

---

Kantian tradition, our moral responsibility for our actions arises on account of our free will. Christine M. Korsgaard, *Morality as freedom*, *in* CREATING THE KINGDOM OF ENDS 159, 159 (1996). According to Carter, "[a] rich notion of 'freedom' can be employed to generate a rich morality." Alan Carter, *Morality and Freedom*, 53 PHIL. Q. 161, 177 (2003). As I understand it, a policy measure's moral worth depends upon its impact on autonomy. If it enhances autonomy, then the said regulation is morally worthy.

98 Kammourieh et al., *supra* note 7, at 44.

99 Mokrosinska, *supra* note 31, at 121–22.

100 Trudy Mercadal, *Identity Formation*, SALEM PRESS ENCYCLOPEDIA (2017).

servative."[101] For the purposes of privacy studies, both aspects of an individual's identity—personal and social—are important.

B. Personal Identity

As per John Locke, personal identity is a matter of psychological continuity.[102] For Altman, "self-identity is the ultimate goal of privacy regulation."[103] He defines self-identity as "a person's cognitive, psychological, and emotional definition and understanding of himself as a being. It includes knowing where one begins and ends vis-à-vis others."[104] As per Hogg, Terry, and White, "Identity is the pivotal concept linking social structure with individual action,"[105] hence it becomes important from privacy studies perspective. Agre and Rotenberg state that "control over personal information is control over an aspect of the identity one projects to the world."[106] Unfortunately, the focus of privacy studies is more on identification and less on identity formation.[107] This myopic view is ironic because one cannot protect an individual's identity without understanding the underlying constitutive process. This constitutive process is not limited to personally identifiable information but extends to the larger social identity.

C. Social Identity

While the idea of viewing an individual as a member of a group may be relatively new to the field of privacy studies, this idea is well explored in the realm of social psychology.[108] The Social Identity Theory explores the implications of group membership on an individual's behavior.[109] Tajfel defines social identity as "a person's sense of who they are

---

101 Jaclyn Rodriguez, *Social Identity Theory*, SALEM PRESS ENCYCLOPEDIA (2019).

102 Carsten Korfmacher, *Personal Identity*, INTERNET ENCYCLOPEDIA OF PHILOSOPHY, https://www.iep.utm.edu/person-i/ (last visited Sept. 27, 2020).

103 Irwin Altman, *Privacy: A Conceptual Analysis*, 8 ENV'T & BEHAV. 7, 25 (1976) (emphasizing the role of privacy as an interpersonal boundary control process).

104 *Id.*

105 Michael A. Hogg, Deborah J. Terry & Katherine M. White, *A Tale of Two Theories: A Critical Comparison of Identity Theory with Social Identity Theory*, 58 SOC. PSYCHOL. Q. 255, 257 (1995) (critically analyzing identity theory and social identity theory).

106 PHILIP E. AGRE & MARC ROTENBERG, *Introduction*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 7 (2001) (summarizing the new landscape of privacy).

107 *See* Floridi, *supra* note 19, at 94.

108 *See generally* ROBERT A. BARON, DONN BYRNE & JERRY SOLS, EXPLORING SOCIAL PSYCHOLOGY (3d ed. 1989) (defining social psychology as "the scientific field that seeks to understand the nature and causes of individual behavior in social situations.").

109 *See* Henri Tajfel, *Experiments in Intergroup Discrimination*, 223 SCI. AM. 96, 101–02 (1970) (stating that division into groups is enough to trigger discriminatory behavior); *see generally* Henri Tajfel & John Turner, *An Integrative Theory of Intergroup Conflict*, *in* THE SOCIAL PSYCHOLOGY OF INTERGROUP RELATIONS 33 (William G. Austin and Stephen Worchel eds., 1979) (presenting an outline of a theory of intergroup conflict).

based on their group membership(s)."[110] Social identity is the individual's knowledge that they belong to certain social groups along with the emotional significance of this group membership.[111] The social identification resulting from group membership determines one's attributes as a group member.[112] To protect the social identity one must safeguard the constitutive group elements. I explore the relationship between identity and privacy further in the next section.

D. The Relationship Between Identity and Privacy

We need to appreciate that in the age of social networking, big data, and profiling, the relationship between identity and privacy has fundamentally changed. Privacy is no longer merely about access to information or identity theft; it has moved on to the constitution of identity. As Robison states: "It is not as though we own our identity—like we might own a photograph, or clothing, or a car. We are our identity, as it were."[113] Floridi rejects the existing approaches to define privacy as unsuitable for the digital age and highlights the identity-constituting value of privacy.[114] Lampinen notes that an individual's technology preferences are at least partially driven by the need to identify with groups.[115] While drawing on identity theory and privacy research, Wu argues that the need for self-identity is an important factor impacting "people's privacy behavior in social networking sites."[116] Bezanson states that "disclosure of personal information to intimate communities is a necessary precondition to the individual's development of personal and social identity."[117]

---

110 Saul Mcleod, *Social Identity Theory*, SIMPLY PSYCH. (Oct. 24, 2019) https://www.simplypsychology.org/social-identity-theory.html.

111 Hogg, *supra* note 14, at 6.

112 Michael A. Hogg & Deborah J. Terry, *Social identity theory and organizational processes*, *in* SOCIAL IDENTITY PROCESSES IN ORGANIZATIONAL CONTEXTS 3 (MICHAEL A. HOGG & DEBORAH J. TERRY eds., 2001) (providing a basic description of the key features of the social identity theory).

113 Wade L. Robison, *Digitizing Privacy*, *in* CORE CONCEPTS AND CONTEMPORARY ISSUES IN PRIVACY 189, 196 (Cudd & Navin eds., 2018) (analyzing invasions of privacy caused due to digitization).

114 Floridi, *supra* note 19, at 94.

115 ARI LAMPINEN, INTERPERSONAL BOUNDARY REGULATION IN THE CONTEXT OF SOCIAL NETWORK SERVICES 62 (2014).

116 Philip Fei Wu, *The Privacy Paradox in the Context of Online Social Networking: A Self-Identity Perspective*, 70 J. ASS'N FOR INFO. SCI. & TECH. 207, 207 (2019) (presenting a research model illustrating theory of relationship between self-identity and information privacy).

117 Randall P. Bezanson, *The Right to Privacy Revisited: Privacy, News and Social Change, 1890–1990*, 80 CAL. L. REV. 1133, 1147 (1992).

The harmony between personal and social identity, and the recognition of the broader identity in privacy studies[118], that I seek is also in conformity with Erik Erikson's theory of psychosocial development, which states that "individual identity evolves throughout life in balance with broad sociocultural pressures."[119] According to Hogg, Terry, and White, "identity theory postulates that self reflects the wider social structure insofar as self is a collection of identities derived from the role positions occupied by the person."[120] As per Cudd and Navin, "[a] person's social identity or social role can make [them] (or others) more or less vulnerable to harms when [their] privacy is either violated or protected. Accordingly, the value that we grant to privacy depends, at least in part, on the social identities of the people whose privacy concerns us."[121]

The relationship between privacy and identity is socially nuanced, although it is usually understood in the limited context of personal identity. In order to fully comprehend the relationship between identity and privacy, one must evaluate the harm suffered at an identity level on account of violation of privacy. As per Robison, treating individuals as "packets of information" is a violation of their moral autonomy.[122]

An artificial bifurcation of privacy into individual and group privacy cannot protect our autonomy as moral agents. As per Hildebrandt,

> If you define personal information as a set of true facts that identify a person as an individual, you imply a static conception of identity: it presumes that the core of an individual can be fixed for identification (date of birth, nationality, eye [color], gender etc.) . . . [b]ut, unlike identification in the sense of unique [categorization], construction of the identity of the self implies indeterminacy, and privacy therefore implies the recognition of this indeterminacy.[123]

In my opinion, Hildebrandt's views hint at a bridge between individual and group privacy. The determinate personal information falls

---

118 For privacy's conventional focus on personal identity to the exclusion of social identity, see Baskerville, *supra* note 30.

119 Joseph Dewey, *Psychosocial Development*, SALEM PRESS ENCYCLOPEDIA (2019).

120 Michael A. Hogg, Deborah J. Terry, & Katherine M. White, *supra* note 105, at 258–59 (discussing the similarities and differences between identity theory and social identity theory).

121 Ann E. Cudd & Mark C. Navin, *Introduction: Conceptualizing Privacy Harms and Values*, *in* CORE CONCEPTS AND CONTEMPORARY ISSUES IN PRIVACY 5 (2018) (discussing the values of privacy).

122 *See* Wade L. Robison, *Privacy and Personal Identity*, 7 ETHICS & BEHAV. 195, 205 (1997) (discussing how the appropriation of our identities diminishes our standing as autonomous moral agents).

123 Hildebrandt, *supra* note 14, at 51–52.

under the purview of individual privacy and the indeterminate construction of self takes place through social identity and lies under the purview of what is presently considered to be group privacy. Our identities are not limited to merely our personal information. Our social identities are equally deserving of protection under privacy norms and regulations.[124]

V. PRIVACY AND AUTONOMY

Privacy's role is widely recognized in protecting autonomy.[125] However, one needs to be autonomous in order to exercise the right to privacy.[126] How do we resolve this quagmire where privacy is seemingly a precondition for autonomy and autonomy a prerequisite for privacy? The answer lies in analyzing autonomy. What "autonomy" are we referring to when we refer to the relationship between privacy and autonomy? Is it the state of autonomy or the exercise of autonomy?[127] The two have different implications. When privacy facilitates the state of autonomy, it cannot do so as a right—for the state of autonomy is a necessary precondition for the exercise of right to privacy.[128] In such a scenario, the relationship between privacy and autonomy is that of a value at the primary stage.[129] Having attained the state of autonomy, the individual can subsequently exercise their right to privacy autonomously.

The dichotomy of privacy as a social value and a right can be further appreciated through the evolution of the relationship between privacy and autonomy from detachment to social engagement. Whilst the earlier classical liberal view emphasized upon sheltering the individual from the society, contemporary scholarship recognizes the role social relationships play in shaping autonomy and privacy's role in protecting

---

124 The GDPR prescribes regulations for collection and processing information pertaining to social identity. However, it does not prohibit collection, processing, profiling and algorithmic grouping on the basis of such data. *See generally*, European Parliament and Council Directive 2016/680, art. 1, 2016 O.J. (L. 119) (EU). In the ensuing parts, by analyzing the threat Big Data Analytics pose, I argue that the existing regulations are inadequate.

125 Mokrosinska & Roessler, *supra* note 49, at 2.

126 Raz *supra* note 97, at 376.

127 This formulation of autonomy is consistent with Raz's dual account of autonomy, which in a primary sense is the actual living of an autonomous life and in its secondary sense is the capacity to live autonomously. Raz, *supra* note 97, at 372–73.

128 Cohen states, "The self has no autonomous, precultural core, nor could it, because we are born and remain situated within social and cultural contexts." Cohen *supra* note 31, at 1908.

129 *See* Beate Roessler & Dorota Mokrosinska, *Privacy and Social Interaction*, 39 PHIL. & SOC. CRITICISM 771, 774 (2013) (arguing that it is not always reasonable to assume a conflict between individual privacy on the one hand and society on the other). Roessler & Mokrosinska argue "social norms regulating informational privacy not only regulate and facilitate the protection of individual autonomy, but are also necessary for the constitution and regulation of social roles, relationships and, more generally, social practices." *Id.*

these social relationships.[130] Mokrosinska, while summarizing the criticism of the earlier view of autonomy, states,

> (1) [A]utonomy is the ability to direct one's actions from within values and commitments central to one's identity, and (2) people's identities are constituted by a variety of social roles, relations and practices then (3) the exercise of autonomy cannot demand detachment from social life. Detachment from those social elements central to one's identity would alienate one from one's core commitments and, hence, undermine one's autonomy.[131]

Privacy makes the exercise of individual autonomy meaningful by protecting its surrounding social contexts.[132] Therefore, the more socially enhanced the role of the individual, the more enhanced privacy will be as a social value.

A. Privacy as a Social Value

The social value of privacy is well recognized under privacy scholarship.[133] The focus is usually centered on the instrumental value of privacy and the role it plays in fostering social relationships.[134] As Schoeman notes, "[t]he practice of privacy, not as a right but as a system of nuanced social norms, modulates the effectiveness of social control over an individual."[135] I agree with much of the scholarship on the issue. However, instead of focusing on the value of privacy, I examine privacy *as* a value—specifically as a social value (P_v).[136] I believe this is necessary to explain the evolution of privacy from a value to a right and the relationship between privacy and autonomy. While analyzing privacy as a social value, I do not discard its importance as a moral and political

---

130 *See* Mokrosinska, *supra* note 31, at 117.

131 *Id.* at 121–22.

132 *See id.* at 123.

133 Regan, *supra* note 16, at 50.

134 *Cf.* Kirsty Hughes, *The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 225 (Roessler and Mokrosinska eds., 2015) (discussing the ways in which privacy is beneficial to the society). Hughes notes "[T]he term 'social value of privacy' remains puzzling, in part because it is used in several connected and overlapping senses. The first is the idea that privacy is a common good, the second is to discuss the value of privacy to society and the third is to reclaim the socializing function of privacy." *Id.* (emphasis omitted).

135 FERDINAND D. SCHOEMAN, PRIVACY AND SOCIAL FREEDOM 6 (1992); *see also* Regan, *supra* note 16, at 54 (discussing Schoeman's stance on the social importance of privacy).

136 *See* MILTON ROKEACH, THE NATURE OF HUMAN VALUES 5 (1973). As per Rokeach, "A value is an enduring belief that a specific mode of conduct or end-state of existence is personally or socially preferable to an opposite or converse mode of conduct or end state of existence." *Id.*

value. However, for the purposes of this Article, in line with the group nature of privacy, I restrict my analysis to privacy as a social value.

Since 1990s, the social value of privacy has been the focus of privacy scholarship in various forms. As per Regan, "[a]cceptance of the self as 'socially constructed' provides what may be considered as a macro-level confirmation for the social value of privacy."[137] Privacy is important for an individual's functioning in society.[138] Fischer-Hübner and others have noted that privacy, apart from being an individual right, is also a societal good which underlies values such as democracy and pluralism.[139] Analysis of privacy as a social value also highlights an underlying interdependence in protection of privacy. Hildebrandt notes, "[w]ithout shelter, without fellow human beings who respect our unwillingness to share private thoughts, and without a legal system that gives us an effective right to ward off intrusions into our private life, we have no privacy."[140] Hence, it would be incorrect to construe privacy merely as an individual right and not also as a social value. Raz's assertion of autonomy being dependent upon realization of a number of collective goods further buttresses privacy's status as a social value.[141] The individual autonomous self is socially embedded and must be protected by recognizing privacy as a social value.

As per Schumpeter, social value "expresses the fact of mutual interaction and interdependence between individuals and the results thereof."[142] When I term privacy as a social value, I acknowledge it to be a value shared socially by the people. It is an acknowledgment of its role in facilitation of social interaction. As I understand it, privacy as a social value plays a pivotal role not only in the formation of the socially autonomous self and the social identity of an individual but also in the functioning of the social groups. The expansive understanding of identity, autonomy and privacy as a social value as enumerated in the foregoing

---

137 Regan, *supra* note 16, at 57.

138 *See id.*

139 Simone Fischer-Hübner, Chris Hoofnagle, Ioannis Krontiris, Kai Rannenberg & Michael Waidner, *Online Privacy: Towards Informational Self-Determination on the Internet*, 1 DAGSTUHL PERSP. WORKSHOP 1, 3 (2011) (raising awareness about the actual state of the art of online privacy). While Fischer-Hübner et al. makes the argument in the European context, this interpretation of privacy is, in my opinion, not culture-specific but universal.

140 Mireille Hildebrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, 20 THEORETICAL INQUIRIES IN L. 83, 84 (2019) (arguing for an understanding of privacy that is capable of protecting the incalculable about the individual in the age of big data analytics.).

141 In the conclusion, I briefly present my formulation of mutual privacy, which recognizes the collective interest in privacy. However, its fuller articulation is subject matter of a subsequent article.

142 Joseph Schumpeter, *On the Concept of Social Value*, 23 Q. J. ECON., 213, 218 (1909) (discussing the meaning and role of social value).

parts forms the basis of my formulation of a group right to privacy which I develop in the next section.

VI. PRIVACY: FROM VALUE TO GROUP RIGHT

The first half of this Article laid the groundwork for developing an expansive account of privacy. I now develop the theoretical framework of privacy as enumerated in the introduction. In the preceding sections, I have provided an account of privacy as a social value. I now focus on transition of privacy from value to individual and group right. Since privacy studies have already explored the conventional individual right to privacy (IRP), here, I develop a novel account of group privacy which can protect the social identity and the socially embedded autonomous self.

As stated in the introduction, my GRP formulation proceeds broadly on the dual lines of the right of an individual as a member of a group and the right of the group itself. This formulation is consistent with Ritchie's account of metaphysics of social groups.[143] Epstein summarizes Ritchie's approach as divided into organized groups that are realizations of structured sets of nodes that stand in a functional relation to one another and feature groups that are collections of people who have a property or feature in common with one another.[144] Feature groups are social groups such as race and gender.[145] Organized groups are groups like clubs and committee.[146]

A. *A Primer to the Triumvirate Formulation of the Group Right to Privacy*

The first form of group right to privacy vests in an individual on the basis of their membership in a social group. Critics of an individualistic right to privacy who highlight its social, political, and technical limitations would support the formulation of this group right to privacy, that an individual holds on the basis of membership in a group. As stated earlier, I also contend that under certain circumstances, another group right to privacy may also exist that is held by the group itself. For ease of reference, I address these two formulations as GRP_1 and GRP_3 respectively.

---

143 *See* Katherine Ritchie, *What are Groups?*, 166 PHIL. STUD. 257, 257–60 (2013) (offering a substantive answer to the question "what are groups?"); *see also* Katherine Ritchie, *The Metaphysics of Social Groups*, 10 PHIL. COMPASS 310, 314–17 (2015) (examining key metaphysical questions regarding groups); Brian Epstein, *What are Social Groups? Their Metaphysics and How to Classify Them*, 196 SYNTHESE 4900, 4904–07 (2017) (presenting a systematic approach for analyzing and explaining the nature of social groups).

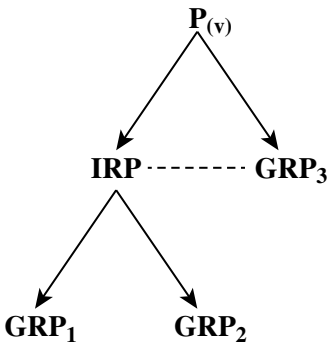
144 Brian Epstein, *Social Ontology*, *in* STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta ed., 2018).

145 *Id.*

146 Ritchie (2015), *supra* note 143, at 310.

Group privacy as it pertains to these two forms of social groups classifies as GRP_1 in case of Feature Groups (e.g., nationality) and GRP_3 in case of Organized Groups (e.g., a reading group). I will also explore an individual's right not to be algorithmically grouped by Big Data Analytics in the form of GRP_2.

Human rights are grounded in values.[147] The group right to privacy is grounded in privacy as a social value. In consonance with my theme of expansion of privacy, I focus on GRP_1, GRP_2 and GRP_3. To this end, I propose a model that I will be explaining in the ensuing paragraphs:



This model focuses on the evolution of privacy as a social value ($P_{(v)}$) into IRP, GRP_1, GRP_2 and GRP_3. In this scenario, $P_{(v)}$ develops into IRP and, on account of social identity, IRP extends into GRP_1. GRP_2 represents the individual's right against algorithmic grouping, which is steeped in their right to informational self-determination. $P_{(v)}$ in certain cases can also be the foundation of GRP_3. One interpretation of this model could be that when it comes to privacy one must treat the individual (IRP) the same as the group (GRP_3) the same, i.e., one can apply the same touchstones of protection of autonomy, identity, and information to the group in the same manner that one can apply them to the individual. However, it is important to note that GRP_3 represents groups created out of devolvement of autonomy by individuals. The indirect relation arising out of the creation of groups when individuals devolve autonomy is represented through the dotted line between IRP and GRP_3. As stated earlier, the distinction between GRP_1 and GRP_3 is constituted in feature

147 *See* John Tasioulas, *On the Foundations of Human Rights*, *in* PHILOSOPHICAL FOUNDATIONS OF HUMAN RIGHTS 45 (Rowan Cruft, S. Matthew Liao, & Massimo Renzo eds., 2015) (distinguishing the contention that human rights have foundations, a version of from certain foundationalist deformations); *see also* Thomas Nagel, *Personal Rights and Public Space*, 24 PHIL. & PUB. AFF. 83, 86 (1995) (stating that rights are a nonderivative and fundamental element of morality). Nagel states, "On the instrumental account, rights are morally derivative from other, more fundamental values: the goods of happiness, self-realization, knowledge, and freedom, and the evils of misery, ignorance, oppression, and cruelty." *Id.*

groups and organized groups. One can understand the difference between the two in terms of voluntary constitution. It stands to reason that, in the case of organized groups, there is a voluntary devolvement of autonomy from the individual to the group, whereas in case of feature groups, an individual is usually born into the group and their enrollment in the group is usually not an exercise of autonomy. I will address all the three group rights in the subsequent paragraphs. In the next section, I begin with my exposition of GRP_1, which protects the individual's social identity and socially embedded autonomous self.

VII. GRP_1

In the age of Big Data Analytics and Covid-19 Apps, the right to privacy, in order to be effective, must meaningfully protect the individual's social identity and socially embedded autonomous self. However, the conventional conception of the right to privacy has been narrowly categorized as the right to be left alone.[148] The edifice of the regulatory device Personally Identifiable Information (PII) is built on the basis of this narrow understanding.[149] Instead of correcting the problem at the level of identity, we have created a category of group privacy to extend the parameters of privacy available to the individual. Similarly, on the basis of a misconstrued account of autonomy, we have understood the primary role of privacy as keeping the individual out of public gaze rather than protecting the social relationships that form the individual.

---

148 Regan, *supra* note 16, at 53.

149 The National Institute of Standards and Technology lists the following as examples of PII:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number
- Address information, such as street address or email address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration number or title number and related information
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Erika McCallister, Tim Grance & Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, NATI'L INST. OF STANDARDS & TECH. (2010) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

GRP_1 seeks to correct this error by protecting the individual's social identity and socially embedded, autonomous self. The privacy problem arising out of Big Data Analytics can be solved by realizing that an individual's identity is an eclectic mix of individual characteristics and group traits.[150] The failure to realize this has created an artificial divide between individual privacy as traditionally understood and what is presently considered to be group privacy, where in fact there is just one non-dual (*Advaita*)[151] privacy. I contend that PII is divisible into three broad categories: one that is solely individualistic—for example, biometric information; a second containing information pertaining to an individual in their capacity as a member of a group, such as nation, religion, and gender; and a third category, comprising of a mix of both individual and group traits such as name. Individual traits need protecting at the individual level, and group characteristics, at the group level. The mix of the two traits needs protecting at the individual level. This formulation is not aimed at negating group privacy as a right of the group, which I address independently as GRP_3 in part IX. The advantage of the conception of GRP_1 is that it helps us address the limitations of the present conception of the individual right to privacy without entering into debates about groups' ontological status and ability to bear rights.

The existing discourse on group privacy is broadly divisible into two categories:

i. Group privacy is a collection of individual privacy.

ii. Group privacy is an independent phenomenon.[152]

---

150 *See* JOHN C. TURNER, PENELOPE J. OAKES, S. ALEXANDER HASLAM, & CRAIG MCGARTY, *Personal and Social Identity: Self and Social Context* 2 (May 7–10, 1992) (unpublished paper) (on file with Australian National University Research School of Psychology).

151 Since a substantial portion of my theory is aimed at eliminating the false duality between what is conventionally considered as individual and group privacy and establishing an all-encompassing harmonious notion of privacy, I draw inspiration from *Advaita Vedanta,* the non-dualistic school of Indian philosophy. *Advaita* means non-dual. *Vedanta* literally means the last portion of the ancient Indian scriptures *Vedas*. *Vedanta* signifies the essence of *Vedas* and is also known as the *Upanishads.* SWĀMI NIKHILĀNANDA, THE MĀNDUKYOPANISHAD WITH GAUDAPĀDA'S KĀRIKĀ AND ŚANKARA'S COMMENTARY 4, 127 (3d ed. 1949). *Advaita Vedanta* states that the ultimate reality-*Brahman* appears as the world on account of its creative energy (Maya). "The world has no separate existence apart from Brahman. The experiencing self (jīva) and the transcendental self of the Universe (ātman) are in reality identical (both are Brahman) . . . Plurality is experienced because of error in judgments (mithya) and ignorance (avidya)." Sangeetha Menon, *Advaita Vedanta*, INTERNET ENCYCLOPEDIA OF PHILOSOPHY, https://www.iep.utm.edu/adv-veda/. The cause of human suffering is ignorance of existence as consciousness and identification with the body-mind complex. Swami Sarvapriyanada, *Sat Chit Ananda The Philosophy of the Upanishads*, *in* THE VEDANTA KESARI 544, 545 (2012) (explaining the true nature of self as existence, consciousness, bliss). The end of the myth of duality between the individual self and the ultimate reality is the end of suffering. *See* ELIOT DEUTSCH, ADVAITA VEDANTA A PHILOSOPHICAL RECONSTRUCTION 47 (1973).

152 *See* Taylor, Floridi & van der Sloot, *supra* note 8, at 8–9.

My theory of group privacy makes a departure from both formulations. I contend that some aspects of individualistic information arise out of an individual's membership in a group. In this sense, individual and group privacy are both part of the same tenet of privacy. There is no individual and group privacy. There is just one privacy, and it exists at multiple levels. In order to ascertain the locus of privacy, we need to ascertain the locus of information.

My formulation of GRP_1 is based on two key assertions: Firstly, that when we observe an individual, we see an assimilation of social groups rather than one single person; Secondly, that when an individual is seeking privacy, they are not only seeking to protect their personal information, but also information pertaining to their group affiliations.

A. Individual as Member of the Group

When we first meet someone, that person's identity is cloaked in relative anonymity. At this juncture, we may be aware of the person's gender or race. Perhaps we can infer their religious affiliation and economic status. This process of observation and inference is, again, group driven. Our analysis of a relatively anonymous stranger's identity is possible because of the person's voluntary and involuntary participation in many groups and our access to prior information about such groups. As human beings, we are so accustomed to group identification that we are not even consciously aware of it. The process of acquaintance is marked by affixing identification markers on a member of a group, thus making them distinct in our eyes.[153] Every new piece of information shared with us—name, age, nationality, profession, marital status, sexual orientation—is an identification marker that helps us differentiate an individual. The erosion of privacy drives this process of differentiation. The transition from group to individual is a journey through privacy.

Big Data Analytics follows a similar process, only the purpose is not to make acquaintance, but to profile individuals based on their social identities for behavioral targeting.[154] GRP_1 seeks to protect an individual's control over formation of their social identity, which today is

153 Perry Hinton, *Implicit Stereotypes and the Predictive Brain: Cognition and Culture in "Biased" Person Perspective*, 3 PALGRAVE COMM. 1, 2 (Sept. 1, 2017) (describing the unconscious nature of stereotyping).

154 *See* MIREILLE HILDEBRANDT, PROFILING THE EUROPEAN CITIZEN CROSS-DISCIPLINARY PERSPECTIVES 19 (Hildebrandt & Gutwirth eds., 2008). Hildebrandt defines profiling as, "The process of 'discovering' correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category." *Id.* at 19.

largely dictated by online social networks.[155] The absence of effective privacy mechanisms can impede the sharing of information, thus also limiting identity construction.[156] As stated, the panoptic sorting of individuals by Big Data Analytics for behavioral targeting purposes gives rise to epistemic bubbles and echo chambers that impede the formation of an individual's social identity.[157] The manipulation of an individual's social identity formation on the basis of attention metrics[158] of likes, comments and followers violates their individual autonomy. Social identity forms through negotiation of socio-cultural pressures, in which privacy plays a balancing role. An individual trapped in epistemic bubbles and echo chambers on account of behavioral targeting is likely to remain the prisoner of their existing prejudices rather than expand their social identity autonomously.[159] I further address the harm suffered on account of violation of GRP_1 in part X. For present discussion purposes, it suffices to say that profiling and behavioral targeting are not value neutral. Jenkins states, "[a]t the very least, classification implies evaluation, and often much more. Humans are generally not disinterested classifiers. This is spectacularly so when it comes to classifying our fellow humans."[160]

To be human is to be part of a group. One cannot protect the human without protecting the larger group. Gardner defines human rights as rights that we have by virtue of being human.[161] But what does it mean to be human? Fichte states,

---

155 *See* Uur Gündüz, *The Effect of Social Media on Identity Construction*, 8 MEDITERRANEAN J. SOC. SCI. 85, 85 (2017) (demonstrating social media platforms' impact on identity construction).

156 Wu, *supra* note 116, at 210.

157 *See* Nguyen, *supra* note 36, at 142.

158 JOSÉ VAN DIJCK, THE CULTURE OF CONNECTIVITY: A CRITICAL HISTORY OF SOCIAL MEDIA 62 (2013) ("In the 'attention economy,' attention means eyeballs or (unconscious) exposure, and this value is an important part of Internet advertising in the form of banners, pop-ups, and paid ad space on websites."). Christopher A. Summers, Robert W. Smith & Rebecca Walker Reczek, *An Audience of One: Behaviorally Targeted Ads as Implied Social Labels*, 43 J. CONSUMER RES. 156, 157 (2016) (demonstrating that a behaviourally targeted ad can act as a social label even when it contains no explicit labelling information).

159 Daniel Lapsley & Dominic Chaloner, *Post-truth and Science Identity: A Virtue-based Approach to Science Education*, 55 EDUC. PSYCHOLOGIST 132, 137 (2020) ("Individuals who inhabit epistemic bubbles and echo chambers might value forms of inquiry that meet social identity needs to retain the affirmation of a closed epistemic community rather than pursue warranted true beliefs out of respect for the truth.").

160 RICHARD JENKINS, SOCIAL IDENTITY 6 (3d ed. 2008).

161 *See* James Griffin, *Discrepancies Between the Best Philosophical Account of Human Rights and the International Law of Human Rights*, 101 PROCEEDINGS OF THE ARISTOTELIAN SOC'Y 1, 2 (2001) (exploring the discrepancies between the philosophical justifications of human rights and human rights declarations); *see also* John Gardner, *Simply in Virtue of Being Human: The Whos and Whys of Human Rights*, 2 J. ETHICS & SOC. PHIL. 1 (2008) (critically analyzing Griffin's account of human rights).

> The human being (like all finite beings in general) becomes a human being only among human beings; and since the human being can be nothing other than a human being and would not exist at all if it were not this – it follows that, *if there are to be human beings at all, there must be more than one.* This is not an opinion that has been adopted arbitrarily, or based on previous experience or on other probable grounds; rather, it is a truth that can be rigorously demonstrated from the concept of the human being. As soon as one fully determines this concept, one is driven from the thought of an individual human being to the assumption of a second one, in order to be able to explain the first. Thus the concept of the human being is not the concept of an individual—for an individual human being is unthinkable—but rather the concept of a species.[162]

This observation by Fichte succinctly captures the existential essence of being human, the realization of which is unfortunately missing from the existing hyper-individualistic notion of privacy.

B. Group Facets of the Individual

When we seek to protect privacy, we seek to protect the associational linkages between the individual and group attributes.[163] There can be strictly individualistic details such as biometric information which can have privacy implications from genetic perspective, which is a group concern.[164] While it may be possible to protect the linkages with individual attributes at the level of individual privacy, it is impossible to protect the associational linkages with group attributes solely at the individual level. These associational linkages represent an individual's social identity and their socially embedded autonomous self. The group facets of an individual's identity also give rise to interdependence of privacy. Barocas and Levy identify privacy dependencies arising out of participa-

---

162 JOHANN GOTTLIEB FICHTE, FOUNDATIONS OF NATURAL RIGHT ACCORDING TO THE PRINCIPLES OF THE WISSENSCHAFTSLEHRE 37–38 (Frederick Neuhouser ed., 2000).

163 *See* Reuben Binns, *Is There Any Room for Group Privacy?*, *in* ETHICS AND PRIVACY FOR SOCIAL MACHINES, SOCIAL GROUPS AND AGGREGATIONS 10, 12 (2018). While exploring the desiderata for group privacy, Binns notes "Associations between attributes (or sets of attributes) can be learned, even from data which are not sufficient to identify any actual individual." *Id.*

164 Lunshof et al define genetic privacy as "[a]n individual's right—one that is perhaps extended to families and communities—to protection from nonvoluntary disclosure of genetic information. Jeantine E. Lunshof, *From Genetic Privacy to Open Consent*, 9 NATURE REVS. GENETICS 406, 406 (2008).

tion in socially salient groups.[165] GRP_1 can help protect these privacy dependencies.

With this backdrop, we are now in a position to define GRP_1 with the aid of a Razian formulation, which proceeds as, "'X has a right' if and only if X can have rights, and, other things being equal, an aspect of X's well-being (his interest) is a sufficient reason for holding some other person(s) to be under a duty."[166]

C. Definition of GRP_1

In view of the aforesaid analysis, GRP_1 can be defined as: An individual has an interest in protecting their social identity and socially embedded autonomous self, which—other things being equal—is a sufficient reason for holding some other person(s) to be under a duty.

D. Nature of Duty

GRP_1 restricts Big Data Analytics from impinging upon an individual's social identity and their socially embedded autonomous self. However, the *other things being equal* aspect of the formulation means that during the extraordinary course of the pandemic, contact tracing is permissible. But this formulation prevents any secondary usage of the information.

The nature of obligation imposed on the Big Data Analytics by GRP1 can be discharged with an array of possible regulatory measures restricting collection and processing of data pertaining to an individual's social identity. Further measures can include restriction on profiling and algorithmic grouping based on an individual's social identity. These measures are indicative and not exhaustive in nature. Policymakers must test any such policy measure on the basis of its efficacy in protecting an individual's social identity and their socially embedded autonomous self. Before proceeding to the harm an individual suffers on account of violation of GRP_1, I explore the individual's right against algorithmic grouping.

VIII. GRP_2

GRP_2 is the right of the individual *not* to be identified with certain groups. It is a right steeped in informational self-determination. In December 1983, the German Federal Constitutional Court while declaring certain provisions of the revised Census Act unconstitutional enunciated the principle of informational self-determination as "the authority of the individual to decide himself, on the basis of the idea of self-determina-

165 Barocas & Levy, *supra* note 8, at 583.
166 Raz, *supra* note 97, at 166.

tion, when and within what limits information about his private life should be communicated to others."[167] Control over information is the foremost aspect of privacy driven identity formation. Hornung and Schnabel note that privacy and informational self-determination prevent sensitive information from one context (e.g., medical treatment) from proliferating into another context (professional sphere).[168]

GRP_1 protects an individual's social identity by protecting information relating to their membership in social groups. But increasingly an individual's privacy is violated for commercial purposes on account of algorithmically constituted groups that hitherto never existed. Pagallo states, "[r]ather than a unique data subject whose informational self-determination is specifically under attack, individuals will more often be targeted as a member of a group, or as a specimen falling within the set of ontological and epistemological predicates that cluster a group."[169] GRP_2 specifically addresses groups that have been created algorithmically on the basis of a shared activity. This may be based on shopping, online browsing history, clothing preferences, reading choices, etc. The key argument here is: grouping on an arbitrary basis for the purposes of profiling violates the individual's right of informational self-determination. Kammourieh and others highlight the epistemic concerns relating to Big Data's algorithmic group identification as,

> Big Data thus provides new approaches with which groups can be formed . . . Big Data makes the grounds upon which we can identify new groups increasingly imperceptible . . . Groups might no longer be classified based on the perception of certain observers, but through seemingly obscured algorithmic processes. This incomplete awareness of how and on which grounds group identification takes place could lead to an epistemic de-

---

167 Antoinette Rouvroy & Yves Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, *in* REINVENTING DATA PROTECTION? 45 (Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne & Sjaak Nouwt eds., 2009) (elucidating the conceptual relationship between right to privacy and human dignity). *See* BUNDESVERFASSUNGSGERICHT, *Abstract of the German Federal Constitutional Court's Judgment of December 15, 1983* (1983), https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html.

168 Gerrit Hornung & Christoph Schnabel, *Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination*, 25 COMPUTER L. & SECURITY REV. 84, 85 (2009) (examining the population census decision and the German concept of informational self-determination).

169 Ugo Pagallo, *The Group, the Private, and the Individual: A New Level of Data Protection?*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 159, 168 (Linnet Taylor, Luciano Floridi, & Bart van der Sloot eds., 2017) (analyzing the collective and corporation form of group rights).

> pendence on processes we might no longer fully understand.[170]

While it is beyond the scope of this paper to address this issue, it is worth noting that this epistemic darkness diminishes the right to explanation and judicial recourse against any injustice arising out of algorithmic grouping.[171] As stated earlier, algorithmic grouping is a violation of the right to privacy which is based in human dignity.[172] Algorithmic grouping further violates individual autonomy, which permits individuals to determine their own group membership and the consequences thereof. For instance, to profile individuals based on their like or dislike of curly fries as one of the psychometric indicators of a high IQ is, per se, an affront to human dignity and individual autonomy.[173] Taylor states, "[i]f groupings created through algorithms or models expose the crowd to influence and possible harm, the instruments that have been developed to protect individuals from the misuse of their data are not helpful."[174] She further highlights the risk of this kind of predictive modelling, which may result in blurring of categories and consequent viewing of people according to their propensity, rather than as individuals.[175] Wachter has highlighted the challenges posed by affinity profiling- "grouping people according to their assumed interests rather than solely their personal traits" by the online advertising industry.[176] She cautions, "[i]f users are segregated into groups and offered or excluded different products, services, or prices on the basis of affinity, it could raise discrimination issues."[177]

Algorithmically sorting an individual based on surveillance of their online activity violates GRP_2. Tracking cookies, which create a detailed profile of an individual for advertisement purposes, are chief violators in

---

170 Kammourieh et al., *supra* note 7, at 43.

171 *See* Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18, 21 (2017) (arguing that a right to an explanation in the GDPR is unlikely to present a complete remedy to algorithmic harms).

172 Kammourieh et al., *supra* note 7, at 43.

173 *See* Michal Kosinski, David Stillwell & Thore Graepel, *Private Traits and Attributes are Predictable from Digital Records of Human Behavior*, 110 PROC. NAT'L ACAD. SCI. 5802, 5804 (2013) (showing how Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes).

174 Taylor, *supra* note 50, at 14.

175 *Id.* at 42

176 Sandra Wachter, *Affinity Profiling and Discrimination by Association in Online Behavioural Advertising*, 35 BERKELEY TECH. L.J. (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3388639.

177 *Id.* at 7.

this regard.[178] It would be inconceivable for many of the targeted individuals that, for commercial exploitation purposes, they are members of algorithmic groups curated by tracking cookies on the basis of their online shopping history or browsing history. A significant aspect of such algorithmic groups is that their existence is per se a violation of an individual's privacy interests. The fact that such groups may anonymize the profile of the concerned individual is no defense. As stated earlier, even when an individual is not identifiable, they would still remain reachable.[179] These algorithmic groupings even in their anonymized state give rise to privacy dependencies, which Barocas and Levy highlight as privacy dependencies arising out of participation in "non-socially-salient" groups.[180] GRP_2 can protect these privacy dependencies.

There is a key difference between how I envisage GRP_2 and how existing scholarship envisages algorithmically constituted groups from privacy perspective. Kammourieh and others treat algorithmically constituted groups as "passive groups," (i.e., groups that are unaware of their existence and as such cannot be subject matter of rights).[181] They specifically state,

> Where a group cannot be given control over its data (because there is no structured group with capacity to exercise that control), the goal should be to protect the group's essential interests—primarily, its safety—at the analysis and targeting stages, by anticipating and regulating the riskiest uses of data. Where there is no legal subject to benefit from a privacy right, one solution may be to simply guard against harmful abuses of available data by other stakeholders.[182]

So, as per Kammourieh and others, a non-self-aware algorithmic group cannot take the requisite measures to protect its privacy interests. That's a hard proposition to dispute. Hence, I shift the locus upstream. In my opinion, by the time the algorithmic group is constituted, the privacy violation has already occurred.

The creation of the group is itself an act of violation of privacy. Instead of focusing on how a passive group will exercise the right to privacy, we must focus on the fact that the creation of the passive group

---

178 Chris Jay Hoofnagle, Ashkan Soltani, Nathaniel Good, Dietrich J. Wambach & Mika D. Ayenson, *Behavioral Advertising: The Offer You Can't Refuse*, 6 Harv. L. & Pol'y Rev. 273, 273 (2012) (arguing that consumer privacy interventions can enable choice).

179 Barocas & Nissenbaum, *supra* note 6, at 45.

180 *See* Barocas & Levy, *supra* note 8, at 585–86.

181 Kammourieh et al., *supra* note 7, at 55.

182 *Id.*

violates the right to privacy and the right to informational self-determination.

A. *Definition of GRP_2*

In view of the aforesaid analysis, GRP_2 can be defined as: An individual has an interest in informational self-determination and against algorithmic grouping, which other things being equal is a sufficient reason for holding some other person(s) to be under a duty.

B. *Nature of Duty*

GRP_2 restricts Big Data Analytics from grouping an individual algorithmically and impinging upon an individual's right to informational self-determination. However, the *other things being equal* aspect of the formulation would permit contact tracing during the extraordinary course of the pandemic. But this formulation would prevent any secondary usage of the information.

Before proceeding to the harm suffered on account of violation of GRP_2, I briefly analyze the right to privacy as a group right, which is not reducible to an individual right.

IX. GRP_3

GRP_3 is the privacy right of the group, which is not reducible to the right of its individual members. While GRP_3 seeks to protect a group interest, it can also serve as an additional layer of protection for individual privacy.[183] For a group right to privacy to exist, it must satisfy the following requirements:[184]

1. *A group exists*: List and Pettit define a group as a collection of individuals who have an identity that can survive changes of membership.[185] As per Jenkins, a group derives its reality from people thinking that it exists and that they belong to it.[186] This realization is important from the perspective of excluding all 'passive groups.'[187] that is groups where members are not conscious of the existence of the group and other members. So, while arguing for GRP_3, I refer to only those organized groups, which have been created by individuals through the devolvement of autonomy and whose members are conscious of the group's existence.

---

183 BLOUSTEIN, *supra* note 18, at 125.

184 For a detailed analysis of desiderata of group privacy see Binns, *supra* note 163, at 11.

185 *See* CHRISTIAN LIST & PHILIP PETTIT, GROUP AGENCY: THE POSSIBILITY, DESIGN, AND STATUS OF CORPORATE AGENTS 31 (2011).

186 JENKINS, *supra* note 160, at 8.

187 Kammourieh et al., *supra* note 7, at 38–39.

2. *There is an independent justification for the group right*: The methodology many current theories of group privacy follow is that since the violation of privacy happens at a group level, we need a group right to privacy.[188] I am not entirely in agreement with this approach. In addition to the violation, one must also define the interest or value one is seeking to protect through the right. If violation is the sole justification for the right, then if the violation disappears or mutates into a different form of violation, the right also disappears. As Binns states, the definition of group privacy must be distinct from its motivation.[189]
3. *The group right should be separate from the individual right:* Binns states that one of the important desideratum for group privacy is that it should not be reducible to individual privacy.[190] As part of the discussion on GRP_1, I have elaborated upon the false duality between aspects of individual privacy and group privacy, which can be eliminated through protection of social identity. In this section, the reference to group privacy is distinct from individual privacy.
4. *What the group is seeking to protect is a "right to privacy":* Binns argues that group privacy should be about groups and their privacy and not some other ethical principle.[191] In many group settings, intellectual property rights (such as corporate trade secrets) protect interests akin to privacy.[192] However, as I elaborate in ensuing paragraphs, there are many organized groups that have an interest in privacy that the law presently does not recognize.[193]
5. *The group can bear the right to privacy*: Groups are well-recognized as bearers of cultural rights.[194] However, there is a peculiar paradox when it comes to right to privacy. Usually, one seeks privacy from a group. It almost seems counterintuitive to seek privacy as a group. As stated earlier, *passive groups* cannot be the bearer of group right to privacy.[195] In this section, I

---

188 Jennifer Jiyoung Suh, Miriam J. Metzger, Scott A. Reid & Amr El Abbadi, *Distinguishing Group Privacy From Personal Privacy: The Effect of Group Inference Technologies on Privacy Perceptions and Behaviors*, 2 PROC. ACM HUM. COMPUT. INTERACTION 1, 3 (Nov. 2018) (empirically establishing group privacy).

189 Binns, *supra* note 163, at 12.

190 *Id.*

191 *Id.*

192 *Id.* at 5.

193 Elizabeth Pollman, *A Corporate Right to Privacy*, MINN. L. REV. 27, 30–31 (2014) (arguing that most corporations in most circumstances should not have a constitutional right to privacy).

194 *See See* Jones *supra* note 20.

195 *See* Kammourieh et al., *supra* note 7, at 43.

will refer to examples of organized groups, which can bear a right to privacy.

6. *The group right to privacy can be exercised:* From a joint responsibility and collective decision-making point of view, it is highly unlikely that a group, under surveillance or constituted for profiling purposes, whose members are not even aware of each other's existence can exercise the right to privacy. Even from a class-action suit perspective, the litigant acts as a representative of an active group, which, in case of privacy, may amount to reducing group privacy to individual privacy.[196] At this juncture, a brief reference may be made to the dichotomy between the state of autonomy and the exercise of autonomy, which was highlighted in earlier passages concerning the individual. Privacy as a social value coupled with the devolvement of autonomy by individual members paves way for the state of group autonomy, which is a pre-requisite for formation of joint intention and collective decision making. This autonomous group subsequently exercises the group right to privacy.
7. *The right to privacy is protecting a "group interest"*: The interest sought to be protected through an exercise of privacy should not be reducible to an individual member's interest, but instead should be a group interest.[197]

A. Necessary and Jointly Sufficient Conditions for GRP_3

In light of this analysis, the necessary and jointly sufficient conditions for the existence of GRP_3 are:

a. A group exists;
b. The group has an interest in privacy;
c. This interest cannot be protected through an individual right to privacy;
d. This interest also cannot be protected through any other group right.[198]

I cull GRP_3 using these necessary and jointly sufficient conditions through two examples in the next section.

---

196 *See* Paul R. Dubinsky, *Justice for the Collective: The Limits of the Human Rights Class Action,* 102 MICH. L. REV. 1152, 1152 (2004).

197 *See* Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J.L. & POL'Y 425, 458 (2011) ("Groups have an interest in the outcome of information revelation that might be distinct from the interests of the individual members of the group. This kind of group harm cannot be prevented by fully informed individual choice, but can be addressed by institutions' or organizations' action on behalf of the group as a whole.").

198 *See* Binns, *supra* note 163, at 14.

B. Examples of GRP_3

Let's consider an example of two groups: first, a reading group in a university, and second, a group composed of volunteers and their supporters who rescue marooned refugees in international waters.[199] The reading group meets frequently to discuss the writings of a particular philosopher X, which is part of their curriculum. The lifeboat rescue group is working against the stated policy of their country, which is strictly anti-refugee. Now let's analyze both the examples.

C. Reading Group Analysis

When members of the reading group order philosopher X's book from an online website, one may use data analytics to make the following inferences:

i. The number of orders placed in a short span of time by users in similar geographical location and through a university IP address indicate a spike of interest in a particular philosopher.
ii. The number of books ordered, say six, are too few to indicate a class.
iii. But since different users have ordered them, it's unlikely that the order is for a library.
iv. Most likely, the order is for a reading group.

This analysis may reveal the existence of a reading group in a particular university without revealing the details of its members who may still remain anonymous without further corroboration of data. So, if the website becomes aware of the existence of this group is this a violation of GRP_3? The answer must be "no," as the group has no interest in its privacy. There may be an individual interest in privacy, but certainly not GRP_3.

Now, let's take the example further, let's say that the website sensing the presence of this reading group raises the price of philosopher X's books for the next semester. Is this a violation of GRP_3? I would again answer no. Any group privacy claims at this stage can be reduced to individual claims.

Now, let's move away from the website. While studying together in a room, a non-member who enters the room unannounced suddenly interrupts the reading group. Is this a violation of GRP_3? Perhaps. But one could again argue that the group right here is reducible to an individual right to privacy. Although, this rebuttal stands on a weaker ground than the previous ones as group discussions give rise to a distinct group privacy interest.

---

199 For the example of lifeboat rescuers, I am grateful to Katharina Bernhard.

Let's continue further with the analysis. Suppose members of this group have collectively prepared a summary of the writings of Philosopher X. All members have contributed to the analysis. The group members have mutually agreed that only the group's members will have access to this summary. If someone outside the group publishes or copies this summary, we can term it as violation of copyright. But if someone outside the group has merely read this summary, is this a violation of GRP_3? Or can this be reduced to an individual right? At this stage one could contend that this may be a GRP_3 violation because the individual input would be very hard to delineate in the final document, which will make it impossible to determine the extent of individual right. Secondly, even if we were able to delineate the individual input, the individual interest can be said to be limited to that particular portion, so one cannot logically make an individual claim for the privacy over the entire document. Here exists GRP_3.

D. Lifeboat Rescuers

In the case of the lifeboat rescue group example, the volunteers and supporters who are acting out of humanitarian concern know that they are working against the popular sentiment.[200] Hence, the volunteers and their supporters have an interest in keeping the group's existence private. This desire for anonymity is not merely about the membership of the group but the very existence of the group. If the existence of the group becomes public, fewer people would be willing to join or support the group fearing social, political, or legal repercussions. In such an eventuality, the group as a whole is worse off and not just an individual member. In this example, the individual right to privacy or social identity of the individual cannot account for the privacy interest of the group. Here exists GRP_3.

E. Group Autonomy and Group Identity

As I had argued in case of the individual, I make a similar assertion that in case of groups, privacy protects group autonomy and group identity. Langfred notes that autonomy can simultaneously reside at both the group and the individual level.[201] As per Wellman, group autonomy is exercised by a collective as a whole rather than individually by persons

---

200 In *NAACP v. Alabama*, the US Supreme Court held, "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." 357 U.S. 449, 462 (1958); *see also* Pagallo, *supra* note 169, at 165.

201 *See* Claus W. Langfred, *The Paradox of Self-Management: Individual and Group Autonomy in Work Groups*, 21 J. ORG. BEHAV. 563, 563 (2000) (exploring how autonomy at the individual and group levels directly affect group cohesiveness).

in a group.[202] Like in the case of the individual, privacy facilitates the exercise of this autonomy. Privacy assists in the formulation of joint intention,[203] which is required for group decision making. Privacy also lays the foundation for the formation of trust,[204] which is necessary for the group to function effectively. Privacy is a *sine qua non* (which is to say, an essential condition) and an integral part of the group processes.

According to McDougall, "the group . . . is more than the sum of the individuals, [and] has its own life, proceeding according to laws of group life, which are not the laws of individual life."[205] Group identity is the group's distinctive identity as a collective.[206] As per Worchel and Coutant, group identity "includes the group's boundaries, its beliefs and values, its history, and its reputation within the wider domain of groups."[207] So, one can understand group identity in both intra- and intergroup terms. There is an intragroup identity formation qua group

---

202 *See* Christopher Heath Wellman, *The Paradox of Group Autonomy,* 20 SOC. PHIL. & POL'Y 265, 273 (2003) (exploring the prospects of developing a satisfying account of group autonomy without rejecting value-individualism).

203 *See* LIST & PETTIT, *supra* note 185, at 39. List & Pettit posit that a collection of individuals "jointly intend" to promote a particular goal if four conditions are met:

a. Shared goal.
b. Individual contribution.
c. Interdependence.
d. Common awareness.

Id. I contend that privacy is an essential pre-requisite for exercise of these four conditions. Privacy guarantees the autonomy for formulation of shared goal, determining the extent of individual contribution, facilitating conditions of interdependence and creating common awareness. One can reasonably argue that in the absence of privacy the aforementioned four conditions or joint intention will not exist.

204 Trust is yet another important constitutive element of the formation and functioning of groups. Without trust, members of the group cannot effectively organize themselves and coordinate their activities as a group. The relationship between trust and privacy is under explored. Fried while elaborating upon this relationship succinctly states,

> There can be no trust where there is no possibility of error. More specifically, a man cannot know that he is trusted unless he has a right to act without constant surveillance so that he knows he can betray the trust. Privacy confers that essential right. And since, as I have argued, trust in its fullest sense is reciprocal, the man who cannot be trusted cannot himself trust or learn to trust. Without privacy and the possibility of error which it protects that aspect of his humanity is denied to him.

Charles Fried, *Privacy [a moral analysis]*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 203, 212–213 (Ferdinand David Schoeman ed., 1984) (examining the foundations of the right of privacy).

205 MICHAEL A. HOGG, THE SOCIAL PSYCHOLOGY OF GROUP COHESIVENESS 14 (1992); *see also* WILLIAM MCDOUGALL, THE GROUP MIND 13 (1921).

206 Kelly Bouas Henry, Holly Arrow & Barbara Carini, *A Tripartite Model of Group Identification: Theory and Measurement*, 30 SMALL GROUP RES. 558, 561 (1999) (analyzing the similarities and differences between group identification and related concepts).

207 Stephen Worchel & Dawna Coutant, *It Takes Two to Tango: Relating Group Identity to Individual Identity Within the Framework of Group Development*, *in* BLACKWELL HANDBOOK OF SOCIAL PSYCHOLOGY 461, 463–64 (Michael A. Hogg & R. Scott Tindale eds., 2001) (arguing that viewing groups as dynamic units leads to better understanding of individual identity).

members[208] and an intergroup identity formation qua other groups.[209] Since any formation of identity is necessarily an exercise in information control,[210] privacy facilitates formation and preservation of both these identities.

F. Definition of GRP_3

GRP_3 can be defined as: An organized group has an interest in protecting its identity and autonomy, which—other things being equal—is a sufficient reason for holding some other person(s) to be under a duty.

G. Nature of Duty

GRP_3 restricts Big Data Analytics from impinging upon an organized group's identity and autonomy. However, the *other things being equal* aspect of the formulation would mean that during the extraordinary course of the pandemic, information pertaining to the group's activities

---

208 The associational dependence of individual identity on the group identity may at times result in the group identity becoming salient over individual member identities. For instance, in case of even the most prestigious universities, one is aware of the reputation and ranking of the university but ordinarily the students and public at large are not aware of the identity of the principal or the dean. The fact that organized groups such as corporations and universities are identified at an institutional level rather than the individual is indicative of the group right to privacy regulating information interplay in favor of the group over the individual.

209 The annual ranking of universities provides an interesting insight into intergroup identity formation. Whilst universities are ranked across a number of parameters such as student satisfaction, research output, placement, student-faculty ratio, diversity etc.; the actual entities getting ranked are either departments of the university or the universities themselves. These groups are ranked in accordance with the information shared by them or the information procured from the public domain. As stated earlier, formation of any identity whether group or individual is an exercise in information privacy. The ranking of the universities, in contradistinction to each other, is a classic case of competing group identities shaping each other. University rankings are arguably as much a reflection of objective parameters such as number of publications as well as subjective assessment of the quality of publications. Add to this the impact caused by the manner of presentation of information and you have a complex identity formation process happening at group level qua other groups. For objective and subjective aspects of educational rankings, see Lionel S. Lewis, *On Subjective and Objective Rankings of Sociology Departments*, 3 AM. SOCIOLOGIST 129, 129–31 (1968). Another interesting example in this regard would be social media exchange between Twitter handles of sports organizations such as the ICC and Wimbledon. In case the social media accounts of any of these group gets hacked; it would be incorrect to state that the twitter account of an official spokesperson or representative of the group has been compromised. The only correct statement to be made is that the official twitter handle of that particular group has been compromised. But what is it that gets compromised when a twitter handle gets hacked? It's the group's identity. For exchange between Twitter handles of ICC and Wimbledon, see Jai Bednall, *Best Social Media During Incredible Cricket World Cup Final*, NEWS (July 15, 2019), https://www.news.com.au/sport/cricket/world-cup/best-social-media-during-incredible-cricket-world-cup-final/news-story/dc31c204a8dac74879dfd805c3af5696; Edd Dracott, *ICC and Wimbledon Banter on Twitter After Roger Federer Plays Cricket Stroke*, INDEPENDENT (July 10, 2018), https://www.independent.ie/world-news/and-finally/icc-and-wimbledon-banter-on-twitter-after-roger-federer-plays-cricket-stroke-37099959.html.

210 *See* Floridi, *supra* note 19, at 94.

can be obtained for contact tracing purposes. But this formulation would prevent any secondary usage of the information.[211]

GRP_3 imposes obligations on Big Data Analytics that can be discharged with the aid of similar regulatory measures as suggested for compliance with GRP_1. This marks the completion of the triumvirate formulation of GRP. Before proceeding further, I will highlight the two objectives that the Razian formulation of GRP achieves. Firstly, it facilitates the application of GRP. Secondly, it helps us define the limitations of GRP. As regards the first, an individual certainly has interest in protecting their group affiliations as well as an interest in guarding against reduction of their identity to merely a group affiliation. The GRP formulation protects both these interests. The second advantage of the Razian formulation lies in its ability to define the limits of GRP and balance privacy interests with larger public interests. The *other things being equal* aspect of the Razian formulation can help us create emergency exceptions to GRP. With these objectives in the backdrop, I will explore the harm suffered on account of violating the three GRPs.

X. WHAT IS THE HARM SUFFERED AS A RESULT OF VIOLATION OF GRP?

"We cannot wish for that we know not."[212]

In order to understand the way GRP can protect individual autonomy and identity against Big Data Analytics and Covid-19 Apps, I adopt a counter-intuitive approach. Thus far, I have defined the interests sought to be protected by GRP. In order to show how GRP can safeguard these interests, I cite examples of group privacy violations that go beyond the conventional understanding of individual privacy. So, the analysis loop gets completed in the following manner:

i. There is a recognizable interest in group privacy.
ii. This interest is being targeted at the group level.

---

[211] During the course of the pandemic, various religious gatherings have come under increasing scrutiny for their unwitting role in spread of the virus. In the ordinary course, collection of information regarding their practice of religion and members would constitute a violation of GRP_1 and GRP_3. The extraordinary circumstances surrounding the pandemic may permit a limited exception in this regard. *See* Choe Sang-Hun, *'Proselytizing Robots': Inside South Korean Church at Outbreak's Center*, N.Y. TIMES (March 10, 2020), https://www.nytimes.com/2020/03/10/world/asia/south-korea-coronavirus-shincheonji.html?action=click&module=relatedLinks&pgtype=article; *see also* Sharon Otterman & Sarah Maslin Nir, *New Rochelle, Once a Coronavirus Hot Spot, May Now Offer Hope*, N.Y. TIMES (March 27, 2020), https://www.nytimes.com/2020/03/27/nyregion/new-rochelle-coronavirus.html; James McAuley, *How a prayer meeting at a French megachurch may have led to scores of coronavirus deaths*, WASH. POST (April 1, 2020), https://www.washingtonpost.com/world/europe/how-a-prayer-meeting-at-a-french-megachurch-may-have-led-to-scores-of-coronavirus-deaths/2020/04/01/fe478ca0-7396-11ea-ad9b-254ec99993bc_story.html

[212] VOLTAIRE, ZAÏRE, ACT I, SCENE I (1732).

iii. It can be protected by recognizing and enforcing GRP.

Towards this end, I divide this section into two parts. I first highlight the harm individuals suffer on account of Big Data Analytics, and then I focus on the potential lasting impact of Covid-19 Apps on individual privacy.

A. GRP and Big Data Analytics

In this section, I explore some of the harms that an individual is likely to suffer at the hand of Big Data Analytics on account of violation of GRP. The list is indicative and not exhaustive.

1. Hyper-targeted Political Advertising

In 2016, during the course of the US Presidential Election the CEO of Cambridge Analytica (CA), Alexander Nix, remarked in an interview that CA had modelled the personality of every adult in America—some 230 million people.[213] CA had 4,000 to 5,000 data points on each individual. Using these points, they delivered hyper-targeted and hyper-persuasive messages on social media.[214] Ward notes, "[s]uch messages played to hopes, fears, prejudices, and fancies that message recipients may not, themselves, have even been aware of."[215] Ironically by devising a hyper-targeted political campaign, CA has played a crucial role in highlighting the importance of group privacy and the socially interdependent nature of privacy. In October 2020, the UK's Information Commissioner in her letter to the Digital, Culture and Media and Sport Select Committee noted that CA was not involved in EU referendum beyond some initial enquiries.[216] However, if one needs an example of the potential harm that may occur on account of violation of group privacy, one may consider the following snapshot of the document from CA's presentation

---

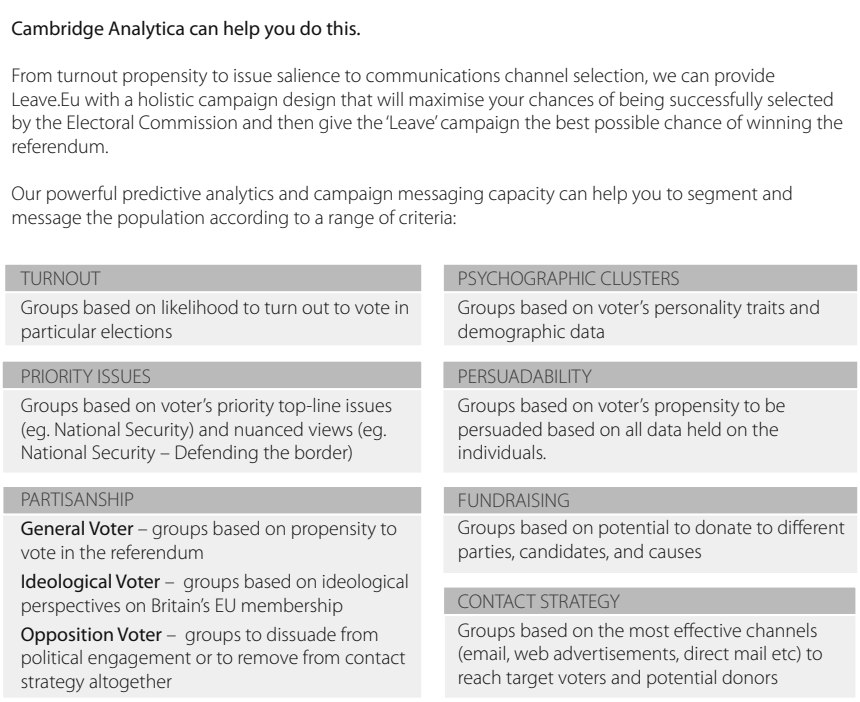
213 Tom Cheshire, *Behind the Scenes at Donald Trump's UK Digital War Room*, SKY NEWS (Oct. 22, 2016), https://news.sky.com/story/behind-the-scenes-at-donald-trumps-uk-digital-war-room-10626155. Notably, Nix made this comment while working on then-candidate Donald Trump's campaign.

214 *See id.*

215 Ken Ward, *Social Networks, the 2016 US Presidential Election, and Kantian Ethics: Applying the Categorical Imperative to Cambridge Analytica's Behavioral Microtargeting*, 33 J. MEDIA ETHICS 133, 133 (2018) (exploring whether Immanuel Kant's categorical imperative could be used by individuals to effectively guard democratic processes).

216 Letter from Elizabeth Denham, UK Information Commissioner, to Julian Knight, Chair of Digital, Culture and Media and Sport Select Committee (Oct. 2, 2020), https://ico.org.uk/media/action-weve-taken/2618383/20201002_ico-o-ed-l-rtl-0181_to-julian-knight-mp.pdf; *see also BBC, Cambridge Analytica 'not involved' in Brexit referendum, says watchdog*, BBC: NEWS (Oct. 7, 2020), https://www.bbc.co.uk/news/uk-politics-54457407.

pitch to Leave.EU.[217] The screenshot of the political campaign proposed by CA seems to focus only on groups and not the individual.[218]



Cambridge Analytica can help you do this.

From turnout propensity to issue salience to communications channel selection, we can provide Leave.Eu with a holistic campaign design that will maximise your chances of being successfully selected by the Electoral Commission and then give the 'Leave' campaign the best possible chance of winning the referendum.

Our powerful predictive analytics and campaign messaging capacity can help you to segment and message the population according to a range of criteria:

TURNOUT

Groups based on likelihood to turn out to vote in particular elections

PSYCHOGRAPHIC CLUSTERS

Groups based on voter's personality traits and demographic data

PRIORITY ISSUES

Groups based on voter's priority top-line issues (eg. National Security) and nuanced views (eg. National Security – Defending the border)

PERSUADABILITY

Groups based on voter's propensity to be persuaded based on all data held on the individuals.

PARTISANSHIP

General Voter – groups based on propensity to vote in the referendum

Ideological Voter – groups based on ideological perspectives on Britain's EU membership

Opposition Voter – groups to dissuade from political engagement or to remove from contact strategy altogether

FUNDRAISING

Groups based on potential to donate to different parties, candidates, and causes

CONTACT STRATEGY

Groups based on the most effective channels (email, web advertisements, direct mail etc) to reach target voters and potential donors

2. Behavioral Targeting

Reduction of an individual's identity to an algorithmic group affiliation is a violation of their autonomy and human dignity. Unfortunately, algorithmic grouping for advertisement purposes has become the chief model of online commercial activities. As per Yan and others, Behavioral Targeting (BT) "refers to the delivery of ads to targeted users based on information collected on each individual user's web search and browsing behaviors."[219] They further state,

---

217 *See* CAMBRIDGE ANALYTICA, LEAVE EU: PROFILE RAISING AND OUTREACH (2015) HTTPS://WWW.PARLIAMENT.UK/GLOBALASSETS/DOCUMENTS/COMMONS-COMMITTEES/CULTURE-MEDIA-AND-SPORT/BK-BACKGROUND-PAPER-CA-PROPOSALS-TO-LEAVEEU.PDF; *see also* HOUSE OF COMMONS DIGITAL, CULTURE, MEDIA AND SPORT COMMITTEE, DISINFORMATION AND 'FAKE NEWS': INTERIM REPORT 27–28 (2018), https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf; *see also* HOUSE OF COMMONS DIGITAL, CULTURE, MEDIA AND SPORT COMMITTEE, DISINFORMATION AND 'FAKE NEWS': FINAL REPORT (2019), https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf (detailing issues around data misuse, data targeting, and Cambridge Analytica).

218 CAMBRIDGE ANALYTICA, *supra* note 217.

219 *See* Yan, Liu, Wang, Zhang, Jiang, & Chen, *supra* note 35, at 261.

> [T]he assumption behind BT is that the users who have similar search or browsing behaviors will have similar interests and thus have higher probability to click the same ad than the users who have different online behaviors. If this assumption is true, *online users can be grouped* into different user segments according to their behaviors for targeted ads delivery.[220]

The Centre for Data Ethics & Innovation (CDEI) defines online targeting as "a range of practices used to analyze information about people and then customize their online experience."[221] The report further states, "[p]ersonalized online advertising enables advertisers to target online advertising to specific groups of people using data about them."[222] Online targeting has a significant downside. For instance, women and people from ethnic minority groups have faced discrimination in the targeting of job ads.[223] In its report on "The Right to Privacy (Article 8) and the Digital Revolution," the UK Parliament's Joint Committee on Human Rights noted that:

> There is a real risk of discrimination "against some groups and individuals through the way this data [is] used": it heard deeply troubling evidence about some companies using personal data to "ensure that only people of a certain age or race, for example, see a particular job opportunity or housing advertisement."[224]

The above instances reveal the dangers of quest for personalization degenerating into compartmentalization of human beings.

3. Discrimination on the Basis of Social Identity

A study conducted by the White House on Big Data notes that web searches tend to discriminate racially on the basis of the name entered.[225]

---

220 *Id.* (emphasis added).

221 CTR. FOR DATA ETHICS & INNOVATION, *Review of Online Targeting: Final Report and Recommendations*, GOV.UK (Feb. 4, 2020), https://www.gov.uk/government/publications/cdei-review-of-online-targeting/online-targeting-final-report-and-recommendations.

222 *See id.*

223 *See id.*

224 JOINT COMMITTEE ON HUMAN RIGHTS, THE RIGHT TO PRIVACY (ARTICLE 8) AND THE DIGITAL REVOLUTION 4, 25 (2019), https://committees.parliament.uk/committee/93/human-rights-joint-committee/news/91474/right-to-privacy-may-exist-on-paper-but-not-in-online-wild-west-says-jchr/

225 EXEC. OFFICE OF THE PRESIDENT, BIG DATA, SEIZING OPPORTUNITIES, PRESERVING VALUES 7 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf; *see also* Latanya Sweeney, *Discrimination in Online Ad Delivery*, 56 COMMUN. ACM 44 (2013) (demonstrating that technology can foster discriminatory outcomes). Benjamin states, "Today the glaring gap between egalitarian principles and inequitable practices is filled with subtler forms of discrimination that give the illu-

The study further points out that when it comes to disadvantaged groups, the challenges from Big Data are not merely limited to privacy but extend to inequitable treatment and loss of autonomy on account of opaque decision making by impenetrable set of algorithms.[226] Ward considers constant scrutiny and sorting of individuals on the basis of internet preferences as akin to Gandy's panoptic sort.[227] When individuals are compartmentalized based on data collected from their everyday lives, it is not only a violation of their autonomy, but this discriminatory technology also limits the opportunities and information available to an individual.[228]

4. Distortion of *Weltanschauung*

The reason online targeting matters is because "it enables people's [behavior] to be monitored, predicted and influenced at scale."[229] The real power of online targeting lies in its ability to shape *weltanschauung*.[230] Imagine two people from remarkably different backgrounds sitting next to each other accessing the same website on their laptops, and the website offers them different content, which the website has customized based on their browsing history. When they open a video streaming website, their choices of "recommended" videos is as much a function of their previous viewing as it is of algorithmic determination based on what "similar" people have viewed. When they access social media, the website pushes different advertisements at them. Two people sitting next to each other in the real world yet panoptically sorted[231] in the virtual

---

sion of progress and neutrality, even as coded inequity makes it easier and faster to produce racist outcomes." Ruha Benjamin, RACE AFTER TECHNOLOGY: ABOLITIONIST TOOLS FOR THE NEW JIM CODE 22 (2019).

226 EXECUTIVE OFFICE OF THE PRESIDENT, *supra* note 225, at 10.

227 Ward, *supra* note 215, at 136; *see also* Gandy, *supra* note 34, at 180.

228 *See* Gandy, supra note 34, at 180.

229 CTR. FOR DATA ETHICS & INNOVATION, *supra* note 221, at 28.

230 Hiebert states, "Worldview is the "fundamental cognitive, affective, and evaluative presuppositions a group of people make about the nature of things, and which they use to order their lives." PAUL G. HIEBERT, TRANSFORMING WORLDVIEWS: AN ANTHROPOLOGICAL UNDERSTANDING OF HOW PEOPLE CHANGE 15 (2008).

Salem Press Encyclopedia's entry on Worldview states,

> Worldview simply refers to the way in which one perceives the world and its inhabitants. It is the lens through which knowledge is filtered. . . . A worldview encompasses perceptions about what is real and what is fictitious. It also defines one's logic and reasoning, such as what the result of an action might be. . . . A worldview is one's perspective of one's place in the world in relation to others. It can be summed up as one's perception of reality.

Renee Butts, *World view*, SALEM PRESS ENCYCLOPAEDIA (2020). Crawford, Miltnet, & Gray note that Big Data "is an emerging *Weltanschauung* grounded across multiple domains in the public and private sectors, one that is need of deeper critical engagement." Kate Crawford, Kate Miltner & Mary L. Gray , *Critiquing Big Data: Politics, Ethics, Epistemology*, 8 INT'L J. COMM. 1663, 1664 (2014).

231 *See* Gandy, *supra* note 34, at 180.

world, this is the result of violation of GRP. A stark example of repercussions of this distortion of reality was visible during the recent attack on U.S. Capitol.[232] In the aftermath of the Capitol Attack, the Center for Humane Technology released a statement highlighting the role of social media in undermining a *shared reality* and noted that "unregulated social media platforms make it impossible for us to see the same set of facts and come to consensus on shared truth."[233]

5. Violation of Privacy on Account of Group Affiliations

Algorithmic grouping does not only distort reality. Egregious examples of such privacy violations include geofencing abortion clinics to target vulnerable women with anti-choice campaigns[234] and targeting young mothers with false anti-vaccine advertisements.[235] Concerted spyware attacks on human rights activists, lawyers, and academics are further examples of GRP_2 violations where malicious actors target an individual's identity on account of a prominent group affiliation.[236] Arguably, such an attack also violates an individual's social identity as attackers target them because of their declared affiliation to a social group. But it is the distinct formulation of groups purely for the violation of an individual's privacy, which makes it a case for violation of GRP_2 as well.

In all the cases of behavioral targeting and discrimination highlighted above, the interest, the right, and the violation are of a group nature. The Razian formulation of GRP is aimed at negating Big Data's zooming and causal power that Part II highlights.[237] One could argue that

---

232 For details of the attack on U.S. Capitol, see Dan Barry, Mike McIntire & Matthew Rosenberg, *'Our President Wants Us Here': The Mob That Stormed the Capitol*, N.Y. TIMES (Jan. 9, 2021), https://www.nytimes.com/2021/01/09/us/capitol-rioters.html.

233 Statement from Center for Humane Technology on Social Media's role in the Attack on the U.S. Capitol (Jan. 8, 2021) https://twitter.com/HumaneTech_/status/1347645673244667905.

234 *See* Sharona Coutts, *Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits*, REWIRE NEWS (May 25, 2016), https://rewire.news/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/.

235 *See* Will Dunn, *Anti-vaccination advert banned—but Facebook still offers targeting of people susceptible to "vaccine controversies"*, NEWSTATESMAN (Nov. 7, 2018), https://www.newstatesman.com/spotlight/healthcare/2018/11/anti-vaccination-advert-banned-facebook-still-offers-targeting-people.

236 *See* David Argen, *Mexico Accused of Spying on Journalists and Activists Using Cellphone Malware*, GUARDIAN (June 19, 2017), https://www.theguardian.com/world/2017/jun/19/mexico-cellphone-software-spying-journalists-activists; *see also* Nick Hopkins & Dan Sabbagh, *WhatsApp Spyware Attack was Attempt to Hack Human Rights Data, Says Lawyer*, GUARDIAN (May 14, 2019), https://www.theguardian.com/technology/2019/may/14/whatsapp-spyware-vulnerability-targeted-lawyer-says-attempt-was-desperate; Stephanie Kirchgaessner, Nick Hopkins & Oliver Holmes, *WhatsApp 'Hack' is Serious Rights Violation, say Alleged Victims*, GUARDIAN (Nov. 1, 2019), https://www.theguardian.com/technology/2019/nov/01/whatsapp-hack-is-serious-rights-violation-say-alleged-victims.

237 STEPHENS-DAVIDOWITZ, supra note 66, at 54.

the violation's impact is felt at the individual level, but it is clear that Big Data targets the individual on account of group interests and affiliations. In order to protect these interests and affiliations, GRP must be invoked, and privacy mechanisms must be deployed at group level in addition to individual.

B. GRP and the Covid-19 Pandemic

In the case of a public health emergency such as the Covid-19 pandemic, GRP would help formulate policy responses at two levels. At the first stage, it would be necessary to identify and quarantine the Covid-19 patients for their treatment as well as safety of others. This formulation is in consonance with the UK's General Medical Council's confidentiality guidelines which state that medical practitioners can disclose patient information in public interest or to prevent potential harm to other individuals.[238] The Razian formulation of GRP permits this identification, with necessary safeguards, for the duration of infection and then restores the balance in favor of the individual's privacy as soon as the health risk abates. The Razian formulation further ensures that the disclosure is on a need basis, and that the PII stays anonymized to the extent possible.

Further, the Razian formulation can help prevent the creation of a new normal in the form of mass health surveillance. As part of their efforts to track the spread of the pandemic and form probable exit strategies from lockdown, countries are increasingly persuading their citizens to download and enroll in public health surveillance apps.[239] Privacy experts have already raised concerns regarding the violation of confidential patient information.[240] But this is a matter of even greater concern from privacy perspective in the post-coronavirus world. From Foucault's perspective, "[f]or the study of human beings, the goals of power and the

---

238 GENERAL MEDICAL COUNCIL, CONFIDENTIALITY: DISCLOSING INFORMATION ABOUT SERIOUS COMMUNICABLE DISEASES (2017), https://www.gmc-uk.org/-/media/documents/gmc-guidance-for-doctors---confidentiality---disclosing-information-about-serious-communica-70061396.pdf?la=EN&hash=354295801490DDF76262B585A680B52DCEB37D8B.

239 *See* Press Release, European Commission, Coronavirus: Commission Adopts Recommendation to Support Exit Strategies Through Mobile Data and Apps, (Apr. 8, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_626; *see also* Alex Hern & Kari Paul, *Apple and Google Team Up in Bid to Use Smartphones to Track Coronavirus Spread*, GUARDIAN (Apr. 10, 2020), https://www.theguardian.com/world/2020/apr/10/apple-google-coronavirus-us-app-privacy.

240 *See* Paul Lewis, David Conn & David Pegg, *UK government using confidential patient data in coronavirus response*, GUARDIAN (Apr. 12 2020), https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response; *see also* David Pegg & Paul Lewis, *NHS coronavirus app: memo discussed giving ministers power to 'de-anonymise' users*, GUARDIAN (Apr. 13, 2020), https://www.theguardian.com/world/2020/apr/13/nhs-coronavirus-app-memo-discussed-giving-ministers-power-to-de-anonymise-users.

goals of knowledge cannot be separated."[241] In the post-pandemic world, there may be great temptations to use the data for secondary purposes.[242] But no matter how laudable the objective, a database which is a living account of the global citizenry's day-to-day existence is inherently dangerous. The post-coronavirus world cannot be built on the edifice of residual surveillance that will result in self-censorship and heightened states of paranoia. GRP's Razian formulation of *other things being equal* ensures that once the epidemic threat subsides, the surveillance efforts cease to exist. The need to decisively end the surveillance effort once the pandemic has subsided can be understood with the aid of "Simveillance"-Simulated Surveillance.[243]

C. Simveillance

In the absence of a moral-legal formulation of the aforesaid triumvirate nature, which are backed by concrete constitutional guarantees, the individual would languish in a state of simveillance.[244] My use of this term in the context of Big Data Analytics and Covid-19 Apps is driven by the extraordinary ambivalence that dictates the participation of an individual in the social sphere in the present age. On one hand, the formulation of the individual's social identity is dependent upon their participation in the online realm. But they cannot do so without being constantly monitored by Big Data Analytics. My concern is that Big Data Analytics's surveillance has become such a "natural" part of the formation of social identity that perhaps in the future we would be unable to form our social identities in its absence. Our internalization of this surveillance means that we would continue to simulate the surveillance, even in its absence, for there never would be a way to conclusively end the skepticism about its existence. In this simulacrum, unlike Bentham's panopticon, even the illusion of surveillance will be unnecessary.[245]

---

241 "In knowing we control and in controlling we know." *See* Gary Gutting & Johanna Oksala, *Michel Foucault*, *in* STAN. ENCYCLOPEDIA PHIL. (Edward N. Zalta ed. 2019).

242 *See* Lauren Kaufman, *Should Public Health Outweigh Data Privacy in Crisis?*, MEDIUM (Mar. 8, 2020), https://medium.com/popular-privacy/coronavirus-is-a-privacy-problem-a396aa44ff88.

243 *See* BOGARD, *supra* note 43, at 4; *see also* Nathan Radke, *Simveillance in Hyperreal Las Vegas*, 2 INT'L J. BAUDRILLARD STUD. (2005), https://baudrillardstudies.ubishops.ca/simveillance-in-hyperreal-las-vegas/. Nathan Radke states, "Simulated surveillance (or simveillance) devices do not allow the observer to actually see the subject; instead, *hyperreal* worlds are created that correspond to the *real* world." *Id.*

244 *See* Radke, supra note 243.

245 *See id.* While distinguishing simveillance from Bentham's panopticon, Radke states: "The reason that the panopticon uses the illusion of constant vigilance is because of the physical problems such vigilance would have posed; Bentham argues that the fiction of observation is as potent as actual observation. When simveillance makes constant vigilance possible, it is no longer necessary to reinforce the illusion of the fiction."

Thus far, I have highlighted the interests that GRP is seeking to protect and some of the harms that an individual is likely to suffer on account of violations of those rights. In the last part, I explore the way forward and argue how the adoption of GRP's Razian formulation and respect for privacy is also in the long-term best interests of the Big Tech corporations.

XI. THE WAY FORWARD. . .

> "I am myself plus my circumstance; and, if I do not save it, I do not save myself."[246]

The conventional conscripted conception of privacy leaves much that is valuable outside the protection of privacy. If GRP_1 is adopted as the standard for privacy regulation, it would help protect the individual's social identity. GRP_3 would provide an additional layer of protection to individual privacy in select cases. As stated, the power of Big Data lies in its ability to zoom in on small subsets of population and conduct highly causal analysis.[247] If the locus of privacy is shifted from IRP to GRP, the shift would negate this power both in terms of collection of data and causal interlinkages. My hope behind writing this Article is the possibility of some of the existing safeguards of privacy that exist at individual level, such as contextual integrity, anonymization, and differential privacy, to be deployed at group level. This would significantly improve the protection afforded to privacy. But this alone will not be sufficient. In order to tilt the scales in favor of privacy, it is imperative to, firstly, show that the mass data collection that is driven by corporate interests lacks any moral justifications and, secondly, that it is in the corporations' best interests to respect privacy in the longer run. I undertake this analysis in the next section.

A. Whose Right is it Anyway?

While my immediate focus is limited to developing a theory of group privacy, in order to test the theory's efficacy, it is important to analyze the larger ecosystem within which this right operates. As things stand today, some consider an individual or group's right to privacy as oppugnant to Big Tech corporations' commercial interests. But is this formulation of privacy versus commercial interests correct, desirable, or even necessary?

One can raise an argument against my formulation of GRP_2 that the revenue generated by targeted advertisement drives the present model of

---

246 JOSÉ ORTEGA Y GASSET, MEDITATIONS ON QUIXOTE 45 (1961).

247 STEPHENS-DAVIDOWITZ, *supra* note 66, at 54.

relatively free access to the various websites on the World Wide Web.[248] Hence, an overreach of privacy concerns would mitigate the benefits that the free access to the leading websites accrues to billions of people across the world.[249] So, the websites' users trade their data in lieu of free access to the websites. This trade-off provides legitimacy to the data practices of Big Tech Corporations. This argument needs to be debunked at multiple levels:

Firstly, it is incorrect to frame the debate as *Privacy v. Access*. The correct formulation is Access with Privacy. The trade-off setup between privacy and access presumes the absence of Privacy Enhancing Technologies (PET),[250] which provide access to websites while preserving the users' privacy.

Secondly, empirical research has revealed the falseness of this trade-off on account of the lack awareness on behalf of the consumers.[251] A majority of the consumers appear to be engaging in trade-offs because they are resigned to giving up their data.[252]

Thirdly, going by the Razian formulation above, in the case of a privacy trade-off one could argue that an individual does not have an interest strong enough in protecting every type of data—for instance, data relating to something as innocuous as the type of coffee they buy. There is *no aspect of their well-being which is a sufficient reason for*

---

248 *See* Tamara Dinev & Paul Hart, *Privacy Concerns and Internet Use, A Model of Trade-Off Factors*, ACAD. MGMT. PROC. 1 (2003) (focusing on the trade-offs between personal benefits and privacy costs associated with Internet use). *See also* Feng Xu, Katina Michael & Xi Chen, *Factors Affecting Privacy Disclosure on Social Network Sites: An Integrated Model*, 13 ELECTRON COM. RSCH. 151, 151 (2013) (analyzing the key factors affecting users' self-disclosure of personal information).

249 *See* Rani Molla, *The cost of an ad-free internet: $35 more per month*, VOX (June 24, 2019), https://www.vox.com/recode/2019/6/24/18715421/internet-free-data-ads-cost; *see also* Matthew Wall, *Would you pay for an ad free internet?*, BBC NEWS (May 10, 2018), https://www.bing.com/search?q=wall+would+you¶ay+or+an+ad+ree+internet&cvid=1dc91ef80e1046efabda60bfe1091e68&pglt=43&FORM=ANNTA1&PC=HCTS; *see also* Andrew Odlyzko, *Privacy, Economics, and Price Discrimination on the Internet*, *in* ECONOMICS OF INFORMATION SECURITY: ADVANCES IN INFORMATION SECURITY 187 (L. Jean Camp & Stephen Lewis eds., 2004) (arguing that reduction of privacy is motivated by price discrimination); Erik Brynjolfsson & Joo Hee Oh, *The Attention Economy: Measuring the Value of Free Digital Services on the Internet*, THIRTY THIRD INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS 1 (2012) (assessing the full value of these digital innovations through time spent on consumption).

250 *See* Johannes Heurix, Peter Zimmermann, Thomas Neubauer & Stefan Fenz, *A Taxonomy for Privacy Enhancing Technologies*, 53 COMPUTS. & SEC. 1, 1 (2015) (describing a universal taxonomy of PETs).

251 *See* JOSEPH TUROW, MICHAEL HENNESSY & NORA DRAPER, THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION 3 (2015) (suggesting that tradeoff between privacy and benefits is misconstrued).

252 *See id. See also* Shoshana Zuboff, *Facebook, Google and a dark age of surveillance capitalism*, FIN. TIMES (Jan. 15, 2019), https://www.ft.com/content/7fafec06-1ea2-11e9-b126-46fc3ad87c65.

holding some other person(s) to be under a duty.[253] But the stakes significantly increase when Big Tech corporations comb and analyze that data in myriad ways to construct a profile of not just the individual, but others like them. Interdependence of privacy means that such grouping can lead to privacy violations of other unsuspecting individuals.[254] As per Levy and boyd, the current legal framework for privacy is individual centric and hence inadequate to grapple with the networked contexts surrounding personal data.[255] Further, individual privacy is marred by what Barocas and Nissenbaum term as the "tyranny of minority," where "the volunteered information of the few can unlock the same information about the many."[256]

Researcher Aleksandr Kogan "gained access to information from 270,000 Facebook members" through a personality test app, "thisisyouridigitallife," including personal data from users and information on the members' friends' profiles, which finally added to 87 million affected users.[257] Kogan then shared this data with CA.[258] The method of data collection shows how our privacy is inter-connected, interdependent, and inter-related. Further, the fact that a smaller sample size data can be used to behaviorally microtarget a large section of population shows that, in eyes of Big Data Analytics, we are all prototypes waiting to be commercially exploited. Kammoureih and others state, "[w]ith Big Data analysis, an individual's habits and characteristics can increasingly be taken to represent a class of similar individuals and, on their own, suffice to draw conclusions about a group."[259] Put differently, in the eyes of Big Data Analytics, there is no innocuous data extrapolation. The gatherer of the data cannot predict all the usage of the collected data.[260] The journey from preference for curly fries to voting preferences can be covered in a few data points using psychometric profiling.[261] Most importantly, in view of the interdependence of privacy, individual interests get aggregated against commercial interests.[262] This strengthens the Razian formulation in favor of the individual.

---

253 RAZ, *supra* note 97, at 166.

254 Barocas & Levy, *supra* note 8, at 561.

255 Levy & boyd, *supra* note 7, at 1; *see also* Ghosh & Kleinberg, *supra* note 81, at 1.

256 Barocas & Nissenbaum, *supra* note 6, at 61.

257 Ivan Manokha, *Surveillance: The DNA of Platform Capital – The Case of Cambridge Analytica Put into Perspective*, 21 THEORY & EVENT 891, 891 (2018) (analyzing the Cambridge Analytica case in the larger context of surveillance in modern day capitalism).

258 *Id.*

259 Kammourieh et al., *supra* note 7, at 38.

260 *See* PRIVACY PROTECTION STUDY COMMISSION, *supra* note 73. *See also* Schwartz & Solove, *supra* note 73.

261 *See* Kosinski, Stillwell & Graepel, *supra* note 173, at 5802.

262 *See* ALLEN BUCHANAN, THE HEART OF HUMAN RIGHTS 172 (2013) ("To say that it is legitimate to appeal to interests in addition to those of the right-holder in order to justify

Fourthly, I argue that privacy enhancing regulation favors the commercial interests in the longer run. At the moment, the definition of PII in the USA does not expressly include social identity.[263] In EU, GDPR provides for regulation of data pertaining to social identity but does not prohibit its collection and processing.[264] In the absence of a balance between

---

having a legal right does not commit one to the thesis that maximizing aggregate interests is what matters.").

263 For the divide across Atlantic as to what constitutes PII or personal data, see Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 877 (2014). In the United States there is a lack of Federal Information Privacy Law and the various State and sectoral legislations work with different definition and aspects of privacy. The lack of uniformity in definition of PII can be demonstrated by examining some of the prominent examples. The United States Government Accountability Office Report to Congressional Requesters defines PII as, "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

U.S. GOV'T ACCOUNTABILITY OFFICE, PRIVACY: ALTERNATIVES EXIST FOR ENHANCING PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION 1 (2008). Even the broad definition of personal information under the California Consumer Privacy Act, 2018 does not expressly include social identity. Cal. Civ. Code § 1798.100 (2018).

264 The European approach to personal information has been broader based from the beginning. Article 2 of the Directive 95/46/EC defines personal data as

> Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or SOCIAL IDENTITY of that natural person. (Emphasis added)

European Parliament and Council Directive 95/46/EC, art. 2, 1995 O.J. (L. 281/31) (EU). This definition of personal data is in conformity with European Treaty No. 108-Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Article 2 of the Convention 108 defines personal data as 'any information relating to an identified or identifiable individual ("data subject"). E.T.S. No. 108.

Article 4 of GDPR defines 'personal data' as:

> Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or SOCIAL IDENTITY of that natural person. (Emphasis added)

Art. 4, 2016 O.J. (L. 119). Article 5 lays down the principles for processing of personal data. Art. 5, 2016 O.J. (L. 119). It is clear from the above definition that in Europe, the identity of an individual is legislatively understood as a combination of individual unique parameters and shared group characteristics. One would have hoped that with such a wide definition, particularly one accounting for social identity of a person, European Law would have explicitly recognized group privacy. However, Opinion 4/2007 states that, "In general terms, a natural person can be considered as 'identified' when, within a group of persons, [they are] 'distinguished' from all other members of the group." ARTICLE 29 DATA PROT. WORKING PARTY, OPINION 4/2007 ON THE CONCEPT OF PERSONAL DATA 12 (2007). This means that even European law treats personal data as only the final linkage between an individual and the larger

commercial and privacy interests, the online commercial world risks heading towards a "market for lemons."[265] The recent exodus of users from WhatsApp to Signal on account of change in privacy policy is an example of ethical interests coinciding with commercial interests.[266] Empirical studies reveal that obtrusive targeted advertising has a negative effect on website visitors because of privacy concerns.[267] Tucker conducted a study that notes that users were nearly twice as likely to click on personalized ads with enhancement of perceived control over privacy.[268] I don't think it is coincidental that, at this stage of evolution of the online commercial model, the captains of industry are echoing the need for greater regulation and privacy protection.[269] In 2019, Facebook settled a suit the American Civil Liberties Union (ACLU) brought "for bias by allowing advertisers to exclude groups based on race, age and sex from opportunities for housing, employment, or credit."[270] The terms of settlement provided that, "Facebook will take proactive steps to prevent advertisers from engaging in unlawful discrimination when sending job, housing, or credit ads to users of Facebook, Instagram, and Messenger."[271] The global regulatory developments also point towards greater recognition of the individual privacy interest. For instance, the Californian Consumer Privacy Act (CCPA), which came into force on January 1, 2020, provides a Californian consumer with greater knowledge and control over their data.[272] The principles of purpose limitation and data

group. The underlying hypothesis continues to be that individual identity can be protected without protecting the larger socio-economic and cultural spheres that it comprises of. Further, Article 22 limits but does not prohibit profiling. Art. 22, 2016 O.J. (L. 119). Taylor highlights that Big Data Analytics bypass the legislative safeguard by potentially harming individuals without identifying them. *See* Taylor, *supra* note 50, at 19.

265 *See* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488, 488–89 (1970) (analyzing the impact of information asymmetry on the goods traded in a market).

266 Alex Hern, *WhatsApp loses millions of users after terms update*, GUARDIAN (Jan. 24, 2021) https://www.theguardian.com/technology/2021/jan/24/whatsapp-loses-millions-of-users-after-terms-update.

267 *See, e.g.*, Andrea M. Matwyshyn, *Discussion of "Online Display Advertising: Targeting and Obtrusiveness" by Avi Goldfarb and Catherine Tucker*, 30 MKTG. SCI. 409, 409–10 (2011).

268 *See* Catherine E. Tucker, *Social Networks, Personalized Advertising, and Privacy Controls*, 51 J. MKTG. RES. 546, 546–47 (2014); *see also* Avi Goldfarb & Catherine Tucker, *Online Display Advertising: Targeting and Obtrusiveness*, 30 MKTG. SCI. 389, 400 (2011) (empirically exploring the influences on effectiveness of online advertising).

269 Sundar Pichai, *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, N.Y. TIMES (May 7, 2019), https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html.

270 CTR. FOR DATA ETHICS & INNOVATION, *supra* note 221.

271 Press Release, American Civil Liberties Union, Facebook Agrees to Sweeping Reforms to Curb Discriminatory ad Targeting Practices (Mar. 19, 2019), https://www.aclu.org/press-releases/facebook-agrees-sweeping-reforms-curb-discriminatory-ad-targeting-practices.

272 The CCPA guarantees the following right to California consumers,

minimization, as recognized under Article 5 of the GDPR, can also be said to be aimed at balancing the trade-off between privacy and access.[273]

In view of this analysis, two key takeaways emerge: the individual has a strong moral and legally enforceable interest in protecting GRP, and it is also in the long-term best interests of the Big Tech Corporations to respect GRP. The above-stated regulatory offshoots point towards a healthy trend where the trade-off between privacy and access is sought to be resolved in favor of the individual. A decisive tech regulatory step in this regard can be shifting the global default privacy setting to opt-in instead of opt-out.[274] Fairfield and Engel state, "in the absence of public-

---

- "The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA rights."

STATE OF CAL. DEP'T OF JUSTICE: OFFICE OF THE ATT'Y GEN., *California Consumer Privacy Act (CCPA)*, https://oag.ca.gov/privacy/ccpa.

[273] Art. 5 GDPR Principles relating to processing of personal data

1. "Personal data shall be:
   a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
   b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
   c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data [minimization]');
   d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
   e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) subject to implementation of the appropriate technical and [organizational] measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
   f. processed in a manner that ensures appropriate security of the personal data, including protection against [unauthorized] or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or [organizational] measures ('integrity and confidentiality').
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')"

Council Directive 2016/679, art. 5, 2018 O.J. (L 127) 1.

[274] *See* Lauren Kaufman, *To Opt-In or Opt-Out?*, MEDIUM (Mar. 6, 2020), https://medium.com/popular-privacy/to-opt-in-or-opt-out-5f14a10bae24 ; *see also* Chad Wollen, *Opt in,*

policy attention to privacy's group dimension, individual consumers have been left to negotiate, unsuccessfully, with companies over the use of their data."[275] An important result of the Razian formulation of GRP and the resultant analysis is that the onus now shifts to Big Tech firms to justify their all-pervasive data collection, processing, and analysis practices.

In this Article, through a theoretical model, I have provided a holistic overview of privacy in the age of Big Data Analytics and Covid-19 Apps from social value to group right. Raz states, "Liberal tradition is not unequivocally individualistic, and that some of the typically liberal rights depend for their value on the existence of a certain public culture, which their protection serves to defend and promote."[276] In a similar vein, my construction of GRP and the ensuing Razian formulation is not driven merely by individual interests. Various scholars have elaborated upon the social value of privacy,[277] the interdependence of privacy,[278] as well as privacy as a public good.[279] Building upon this foundation, I wish to assert that in the age of Big Data Analytics, privacy as a right can no longer be exercised meaningfully individually. Our privacy is not only interdependent in nature, but also existentially, cumulatively interlinked. It increases in force with each successive protection.[280] In a cynical yet realistic way, we must be grateful for the privacy challenge posed by Covid-19 Apps and Big Data Analytics. The privacy challenge posed by Covid-19 Apps has helped us realize that while limited exceptions to privacy may be carved out in grave emergencies, there is no moral justification for round the clock surveillance of an individual's existence by Big Data Analytics. Similarly, the threat to privacy posed by Big Data Analytics has helped us realize that privacy was wrongly focusing on the distinguishing aspects of the individual. It is our similarities that are truly worth protecting. These similarities can be protected by recognizing our

opt out - consent is what it's all about, IAPP (Oct. 31, 2018), https://iapp.org/news/a/opt-in-opt-out-consent-is-what-its-all-about/.

275 Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 392 (2015) (explaining why privacy has aspects of public good).

276 RAZ, *supra* note 97, at 245.

277 *See, e.g.*, Regan, *supra* note 16, at 50.

278 *See* Barocas & Levy, *supra* note 8, at 555; *see also* Levy & boyd, *supra* note 7, at 1–2.

279 Privacy as a public good is non-excluding and non-rivalrous. *See* Fairfield & Engel, *supra* note 275, at 387; *see also* Dennis D. Hirsch, *Privacy, Public Goods and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel*, 65 L. J. ONLINE 67, 71 (2016); *and* Priscilla M. Regan, *Response to Privacy as a Public Good*, 65 DUKE L.J. 51, 51–52 (2015).

280 For network effects relating to privacy, *see* MacCarthy, *supra* note 197, at 504; *see also* Gergely Biczók & Pern Hui Chia, *Interdependent Privacy: Let Me Share Your Data*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY LECTURE NOTES IN COMPUTER SCIENCE 338, 338–39 (Ahmad-Reza Sadeghi ed. 2013).

Mutual or Companion privacy.[281] Mutual or Companion privacy means that not only is our privacy interdependent, but in fact a significant portion of my privacy resides in yours.

The only way of ensuring my privacy is by saving your privacy. The greater privacy you will have, the more privacy I will have.[282] In the age of Big Data Analytics, there is a high probability that we belong together either in a feature group, an organized group, or an algorithmically constituted group for computational and profiling purposes. Hence, the GRP formulations proposed in this Article can be an effective measure for protecting our mutual privacy. Counter-intuitive as it may sound, in the age of Big Data Analytics, privacy is something which we have more together.

---

281 The idea of Mutual Privacy or Companion Privacy is inspired by mutual symbiotic relationships and companion plantation. Santos & Reis state, "Mutual symbiosis occurs when both partners get advantages from the association." Carla A. Santos & Alberto Reis, *Microalgal Symbiosis in Biotechnology*, 98 APPLIED MICROBIOLOGY BIOTECHNOLOGY 5839, 5839 (2014). Similarly, Parker et al. define companion planting as "one specific type of polyculture, under which two plant species are grown together that are known, or believed, to synergistically improve one another's growth." JOYCE E. PARKER, WILLIAM E. SNYDER, GEORGE C. HAMILTON & CESAR RODRIGUEZ-SAONA, COMPANION PLANTING AND INSECT PEST CONTROL, WEED AND PEST CONTROL 1 (2013), https://www.intechopen.com/books/weed-and-pest-control-conventional-and-new-challenges/companion-planting-and-insect-pest-control.

282 *See* Fairfield & Engel, *supra* note 275, at 387 ("Your privacy is not yours alone. The data that a person produces concerns both herself and others. Being cautious with personal data is therefore not enough. Individuals are vulnerable merely because others have been careless with their data. As a result, privacy protection requires group coordination. Failure of coordination means a failure of privacy. In short, privacy is a public good.").