UNIVERSITÄT BONN
RHEINISCHE FRIEDRICH-WILHELMS-UNIVERSITÄT BONN

TRA INDIVIDUALS AND SOCIETIES
TRANSDISCIPLINARY RESEARCH AREA

Rethinking Privacy after this Pandemic

Symposium at the University of Bonn

Book of Abstracts

Karen Adkins	Shifting the Paradigm on "Private" Employee Harassment	1
Eike Buhr	Is there a Right to Local Privacy? A Conceptual Analysis of the first Covid Lockdown and its Influence on the Value of Privacy	3
Sergio Genovesi	Digital Rights in Times of Pandemic	6
Claire Ma	Regulating Information Privacy and Technological Change in the American Economy.	7
Leon A. Morenas	India's Tryst with Data Privacy	11
Manohar Kumar	COVID-19 and an Everyday Account of Privacy	13
Danaja Fabcic Povse	Risk Management in the Covid19 Pandemic and its Impact on the Rights to Privacy and Non-Discrimination	15
Chris Zajner	Medical Privacy in the Wake of the 1889 'Russian Flu' Pandemic	16
Peter Zuk	Neural Data: Not for Sale	18

Shifting the Paradigm on "Private" Employee Harassment

Karen Adkins

The COVID pandemic revealed and exacerbated the asymmetry between employers and employees in many white collar professions. Moving office workers into remote work did not eliminate or reduce racist or sexual harassment of employees; rather, it simply moved it onto digital plattorms that were o$en unmonitored and unprotected (Fessler 2021). While a few examples of harassment, such as public figures who exposed themselves to colleagues on work Zoom calls, were subject to momentary notoriety (if few lasting consequences), the structural problems revealed by online harassment deserve more attention, particular by thinking about privacy. My argument here is simple: first, that there is a double standard around harassment of employees at work that crosses boundaries of private space, and second, thinking of the broad range of private harassment of employees at works points away from corporate surveillance remedies, and towards more vigorous, public, and governmental defenses of the scope of employee rights.

Online harassment o$en takes place either in realms outside workplace governance (i.e. because employees are working from home), or on channels, platorms or devices that are not under employer surveillance. But this sort of undocumented or unmonitored employee harassment has long pre-dated remote work for white-collar employees; workers who clean houses, hotels, or work in private homes as nannies or other household employees, have traditionally crossed boundaries of private and public, and have long been subject to racist and sexist harassment, and abuse. In particular, because these workers are overwhelmingly women, and o$en have linguistic or citizenship barriers, their awareness of their rights and status, or sense of efficacy in utilizing those rights and procedures, can be deeply precarious (Yeung 2020). The double standard between how long these private employee violations occurred with no public awareness, and how immediately online employee harassment was publicized as a problem requiring attention, speaks to the ways in which privacy is afforded to those with economic, class, and racial privilege. This suggests that we are paying too much attention to the loss of privacy for those who are traditionally afforded it, and not enough attention to the ways in which some jobs are constructed around a loss of privacy. The loss of privacy from those who are too used to it was shocking, whereas the continual violation of those seen as never worthy of workplace privacy went largely unacknowledged.

Just as this double standard of privacy exists in the recognition of its loss, there seems to be a problematic double standard in conventional solutions to remote employee harassment. Conventionally, and entirely appropriately, discourse around workplace harassment focuses on bureaucratic, procedural, and legal remedies. But because remedies for workplace harassment rely so much on formal documentation and procedures, remote harassment can present as more opaque and less challenge-able. It occurs in a more private zone. Indeed, much of Yeung's journalism focuses on the kinds of challenges that were presented in documenting, tracing, and accounting for the violations house- and office-cleaners experienced, because of the unsurveilled and untracked nature of their workplaces.

Formal and procedural remedies around workplace harassment are of course justified on moral and legal grounds, and should continue. But my worry is that the format of remote employee harassment (online, through Zoom) is driving too much of the focus on response, and inviting

merely technical solutions (namely increased surveillance of employee use of technology). This I think is the wrong move. Increased surveillance would be tempting for managers, because it is technically doable (encourage screenshots, require that online meetings be recorded) and appears to result in transparency. But I want to argue that increased employer surveillance is not an adequate response, using Elizabeth Anderson's work on private government as my model (2017). Anderson makes use of social contract theory to debunk the neoliberal acceptance of minimal restrictions on employer rights to limit employee behavior, including non-compete agreements, nondisparagement clauses, and the like. Anderson argues that when employers have too free a hand with policy-secng and -enforcement, they can operate in an asymmetric fashion that functions more like a dictatorship, and that employees are rendered as subjects rather than participants. Indeed, her critique of the workplace as dictatorship fairly applies to the kinds of precarious employment Bernice Yeung documents.

Both Yeung and Anderson are illustrating the kinds of injustices that result when too much power is concentrated in employer hands, and when structural features limit their transparency and accountability. The workers Yeung interviews are able to achieve remedies first through solidarity with one another (by forming associations or unions), and then through collective court cases (to demonstrate the systemic and pervasive nature of the problem). The remedies they achieve are both financial and procedural, including specific training around these issues and employee rights of redress. Fundamentally, the workers profiled in Yeung's book achieved justice because they asserted their rights as a collective; they insisted on their worth as humans, and that their employers stop treating them as fungible line items in budgets. This, I think, is the additional move required to combat online harassment, in supplement of policies that already exist, and in lieu of technical 'solutions' that would merely still further reduce employee autonomy and dignity. As remote work looks to be increasingly part of work across sectors of employment, the lines of privacy and publicity look to be increasingly blurred in more sectors of work. Rigorous, public, and sustained assertions of employee rights and dignity must be the first step in clearing space for employee protections, even when they occur in private realms.

Is there a right to local privacy? – a conceptual analysis of the first covid lockdown and its influence on the value of privacy

Eike Buhr

As part of the measures to contain the Covid 19 pandemic, citizens in Germany and many other countries were urged to stay in their private homes as far as possible and to leave the house only to go to (system-relevant) work, to go grocery shopping or to visit a doctor. This was intended to prevent the spread of the virus and to protect society from uncontrolled infection. Since many members of society had to work from home, domestic activities that previously took place primarily in private, such as raising children or designing and arranging one's own home, were coming into the public eye. While at the beginning voices could be heard that tried to gain something positive from the lockdown as a deceleration, it quickly became apparent that a deceleration could only occur for those who had enough living space available to be able to continue to (spatially) separate work, child rearing and leisure and who could externalize parts of the care work. Here, a blurring of boundaries between living and working space can be observed. Beyond a possible violation of informational self-determination, the curfews and contact restrictions thus represent an intrusion into local privacy. In the liberal tradition, the value of local privacy - meaning the privacy of the apartment, the room, the home - is seen primarily in withdrawal from and protection against the public sphere and administrative intervention, and in regeneration, individual autonomy, and familial intimacy. Since it was no longer allowed to leave the private home for any purpose or invite people there, the private sphere was now directly subject to political directives, so that the status of local privacy as a regenerative place of retreat and individual autonomy seemed to be in danger of becoming colonized. According to Habermas, colonization means the "disruption of the symbolic reproductions of the lifeworld" (Habermas 1987, 452), which, due to the intrusion of cognitive-instrumental rationality of economy and administration, "takes precedence in other, communicatively structured areas of life [...] and there at the expense of moral-practical and aesthetic-practical rationality" (Habermas 1987, 451).

This raises the question of whether local privacy has lost its presumed value and whether a *colonization* of local privacy has taken place, that is, the organization of this sphere of life according to external norms and requirements. Based on earlier work I will reconsider the concept of privacy developed in Buhr (2020) and discuss the theoretical assumed changes in the perception and management of local privacy in the context of the Corona pandemic in retrospect. This is exemplified by the blurring of boundaries between private living space and public working space as a result from the obligation to remain at home as far as possible. I will argue that the separation between privacy and the public sphere is gender-coded in the liberal tradition and, in the sense of a sexist essentialism, relegates women to domesticity, which has negative connotations in this tradition. Furthermore, it becomes apparent that privacy and the public sphere do not represent completely separate spaces, but rather are to be understood as mutually influencing spheres whose existence and concrete form depend on political regulations and whose relationship affects the basic structure of a society (cf. Rössler 2001, 43; Solove 2008, 92). By elaborating these functions, it will become apparent why privacy is valued and what form of autonomy local privacy is supposed to guarantee.

In Buhr (2020), I argued for not understanding privacy exclusively as a defensive right, but considering more strongly the positive functions of privacy as a regenerative place of retreat and individual autonomy that can be designed and arranged according to individual ideas. Two years later, there is now an opportunity to re-examine the extent to which the infection control measures have affected which of these functions.

The protective measures taken to contain the pandemic have sometimes reinforced the unequal distribution of care work, which resulted in a special burden on mothers and their children (Babore et al. 2021). The fact that even an increase in domestic violence has been recorded shows that the regenerative function of local privacy has turned into its opposite for those affected. In addition, I will explore more strongly the extent to which the housing situation and, in particular, spatial dimensions of housing had an impact on the mental health of individuals during the lockdown (Bower et al. 2021; Groot et al. 2022). Against the background that the perception of the value of local privacy in times of a pandemic increasingly depends on the individual's financial income, since in this context child rearing, work and leisure time sometimes take place not only in the same home but in the same room, it becomes apparent that the value of local privacy, which is primarily coded in gender-specific terms, is now (additionally) undergoing a classist coding. Finally, I will return to the question of the extent to which the measures to contain the infection can be understood as a colonization of local privacy, or whether the need to stay in one's own home as far as possible and the subsequent blurring of the boundaries between private living and public working space have not rather led to an unequal (mental) burden and intensified the inequalities with regard to the housing situation and made them more apparent. Against this background, I will argue for not only considering the above-mentioned positive functions of local privacy more strongly, but also for identifying them as a dimension of the good life. Therefore, the question will be discussed to what extent, in addition to the status of privacy as a right of defense, a positive right of claim to the value of local privacy can be formulated.

References

Babore, Alessandra; Trumello, Carmen; Lombardi, Lucia; Candelori, Carla; Chirumbolo, Antonio; Cattelino, Elena et al. 2021. Mothers' and Children's Mental Health During the COVID-19 Pandemic Lockdown: The Mediating Role of Parenting Stress. In: Child psychiatry and human development. DOI: 10.1007/s10578-021-01230-6.

Bower, Marlee; Buckle, Caitlin; Rugel, Emily; Donohoe-Bales, Amarina; McGrath, Laura; Gournay, Kevin et al. 2021. 'Trapped', 'anxious' and 'traumatised': COVID-19 intensified the impact of housing inequality on Australians' mental health. In: International Journal of Housing Policy 11 (1026), S. 1–32. DOI: 10.1080/19491247.2021.1940686.

Buhr, Eike. 2020. #stayathome als Kolonialisierung der lokalen Privatheit? Eine ethische Auseinandersetzung mit dem Wert des Privaten in Zeiten einer globalen Pandemie. In: ZfPP 7 (2), S. 385–416.

Groot, Jonathan; Keller, Amélie; Joensen, Andrea; Nguyen, Tri-Long; Nybo Andersen, Anne-Marie; Strandberg-Larsen, Katrine. 2022. Impact of housing conditions on changes in youth's mental health following the initial national COVID-19 lockdown: a cohort study. In: Scientific reports 12 (1), S. 1939. DOI: 10.1038/s41598-022-04909-5.

Habermas, Jürgen. 1987. Theorie des kommunikativen Handelns, Band 2: Zur Kritik der funktionalistischen Vernunft. Frankfurt am Main: Suhrkamp.

Rössler, Beate. 2001. Der Wert des Privaten. Frankfurt am Main: Suhrkamp.

Solove, Daniel J. 2008. Understanding privacy. Cambridge, Massachusetts, London, England: Harvard University Press.

Digital Rights in Times of Pandemic

Sergio Genovesi

After two years and a half of pandemic, the global community developed many resources to face the virus and avoid its spread. The use of digital tracing apps has been seen by many observers as very critical and, in many countries where it was not mandatory to install a Corona-App, the majority of the citizens did not download the app since they distrusted either its technical robustness or the use of data that the government and the app provider would have done. One of the major concerns that fuelled the debate was that Corona-Apps would infringe fundamental rights such as privacy. What is at stake is the control of digital data produced by the citizens and their possible misuse by different public or private stakeholders. The talk analyses the debate around the limitation on fundamental (digital) rights to limit the spread of the pandemics.

Full Text: https://www.nomos-elibrary.de/10.5771/9783465145875-345/digital-rights-in-times-of-pandemic?page=1

Regulating Information Privacy and Technological Change in the American Political Economy

Claire Ma

The stunning rise of the information economy in the 20th and 21st centuries inspired a wide-ranging literature on the causes and consequences of this transformation in U.S. political economy. As the U.S. became the seeding ground for successful information technology companies, earlier literature sought to explain the processes of this transformation.[1] Later, as the growth of the information economy dislodged other established industrial and labor market structures, others sought to describe the consequences of this transition.[2] More recently, critics of information technology and its ascendent business models have argued that Internet-based firms have amassed immense market power,[3] destabilized labor market relations,[4] changed state-market relations,[5] profited from an ability to shape human behavior,[6] and built information capacity that might rival that of states.[7]

In the context of considerable public unease over the information economy, the COVID-19 pandemic reignited questions about information privacy and the proper role of both the state and private entities in the surveillance of individuals. Despite the rich interdisciplinary literature on the causes and consequences of this new information environment, the political development of the U.S. government's approach to regulating information privacy has yet to be explored in depth. I argue that in order to "rethink" the future of privacy, we must first examine its history and the reasons for the law's inadequacy. Surveys show that privacy in the U.S. has been a consistent concern for Americans since the 1970s, but this has not translated into any mass mobilization for policy reforms.[8] The policies and laws that govern privacy, on the other hand, are generally of lower salience to the public and less politically controversial than privacy rights writ large. Once we better understand the role that political coalitions -- and especially organized interests within these coalitions -- have played in the evolution of the U.S. regulatory state, we can more accurately imagine what might be possible in our polity's future trajectory.

The contemporary collaboration between the U.S. state and private sector companies in sharing and building information capacity belies the multiple legislative attempts that federal and state governments have taken to regulate the information economy. Although efforts by

---

[1] Saxenian 1994.

[2] Bix 2002; Greene 2021.

[3] Culpepper and Thelen 2019.

[4] Collier et al 2018; Thelen 2018.

[5] Zysman and Breznitz 2012; Cioffi et al 2021; Rahman and Thelen 2019.

[6] Zuboff 2019.

[7] Whittaker 2021.

[8] Bennett 1992: 39, citing the OTA *Federal Government Information Technology,* p. 26; Regan 1995; Newman 2008; Regan 1995: 21,

federal officials during the early days of information technology in the mid-1960s aimed primarily to limit state surveillance, the adoption of computers into public and private organizations stoked fears among both the mass public and public officials about personal privacy and the coercive capabilities that organizations might acquire with centralized information.[9] Legislative decisions to split the regulation of the private sector into separate domains -- thus delineating consumer financial privacy as a different policy problem from patient privacy or children's online safety -- entangled the U.S. in a multi-front battle with multiple policy coalitions to define the scope, design, and enforcement of privacy rights.

The U.S. approach to information privacy policy can be characterized as reactive and cautious ever since the first U.S. information privacy law, the Fair Credit Reporting Act (FCRA), was passed in 1970 to regulate the credit reporting industry. In response to federal efforts to regulate consumer information and to protect consumer privacy, the credit industry mobilized to defend its practices and has consistently lobbied across multiple levels and branches of government to protect and expand the use of consumer scoring throughout the economy.[10] The subsequent failure to pass a comprehensive information privacy law in 1974 led to the further fragmentation of privacy regulations in the private sector, and the mobilization of industry groups throughout the information economy.

Over the next fifty years, the U.S. has struggled to pass and enforce laws to protect legal privacy rights. Often in response to data breaches and privacy violation scandals, Congress debated and legislated privacy in fits and starts. Although the federal government identified health and medical information as a domain in need of privacy regulation during the 1970s, laws to protect patient privacy only entered the legislative agenda during efforts in the 1990s to reform the health care industry. The passage of the Health Insurance Portability and Accountability Act (HIPAA), also called the Kennedy-Kasselbaum Act, in 1996 created one of the most stringent data privacy regimes in the U.S. The law presented barriers to the country's efforts to collect information during the COVID-19 pandemic, leading the U.S. Department of Health and Human Services to waive some of the law's requirements.[11]

In the containing the spread of the pandemic, information privacy during the COVID-19 pandemic was framed as a trade-off between individual rights and communal health. Framing privacy in such a way, however, has characterized the privacy debate in the United States for decades. This circuitous, repetitive pattern of the privacy debate has motivated a new generation of ethicists, legal theorists, and privacy advocates to reimagine privacy as a concept beyond trade-offs and the balance of interests. For those who study politics and policy, however, it is equally imperative to examine the question of privacy empirically, as the product of policy histories shaped by political actors, legal incentives, institutional arrangements, and interest groups strategies.

---

[9] Igo 2018.

[10] Lauer 2017.

[11] Gellman and Dixon 2020.

Privacy advocates often call for the involvement of all stakeholders in privacy reforms, but the identity, role, and preferences of these stakeholders is not always well understood. The mobilization of businesses and trade associations into organized cross-industry groups beginning in the 1970s created a high-stakes policy challenge between privacy advocates and business groups, both of which have tried to regulate privacy without fundamentally disrupting the emergent information economy. It would be a mistake, however, to characterize business groups as a monolithic group. Split along dimensions such as industry type, size, and position in the economy, information industries form varying political coalitions that may lead to different outcomes in regulatory enforcement across the privacy policy domains.

Who shapes the purpose and understanding of privacy rights, who enforces them, and why has policy change to better protect privacy been so difficult to achieve? The information economy is historically and politically constructed as much as it is the result of technological change. By placing information privacy into the trajectory of American political development, privacy can be understood as an understudied case of how political coalitions and government decisions about regulating the economy have long-lasting consequences for individual rights.

References

Bix, Amy Sue. 2002. Inventing Ourselves out of Jobs?: America's Debate over Technological Unemployment, 1929-1981. Baltimore, Md.: Johns Hopkins University Press,. https://babel.hathitrust.org/cgi/pt?id=uc1.32106012397599.

Block, Fred, and Matthew Keller, eds. 2011. State of Innovation: The U.S. Government's Role in Technology Development. Boulder, CO: http://hdl.handle.net/2027/mdp.39076002964695.

Cioffi, John W., Martin Kenney, and John Zysman. 2021. "Platform Power and Regulatory Politics: Polanyi for the 21st Century." SSRN Scholarly Paper ID 3859075. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.3859075.

Collier, Ruth, Veena Dubal, and Christopher Carter. 2018. "Disrupting Regulation, Regulating Disruption: The Politics of Uber in the United States." Perspectives on Politics, January, 919.

Creser, Olivia T. 2021. "In Antitrust We Trust?: Big Tech Is Not the Problem—It's Weak Data Privacy Protections." Federal Communications Law Journal 73 (2): 28.

Culpepper, Pepper D., and Kathleen Thelen. 2019. "Are We All Amazon Primed? Consumers and the Politics of Platform Power." Comparative Political Studies, June. https://doi.org/10.1177/0010414019852687.

Gellman, Robert, and Pam Dixon. 2020. "HHS's Troubled Approach to Waiving Privacy and Security Rules for the Pandemic." World Privacy Forum, September 16, 2020.

Greene, Daniel. 2021. The Promise of Access: Technology, Inequality, and the Political Economy of Hope. Cambridge, Massachusetts: The MIT Press. https://doi-org.proxy.library.upenn.edu/10.7551/mitpress/11674.001.0001.

Igo, Sarah E. 2018. The Known Citizen: A History of Privacy in Modern America. Illustrated edition. Cambridge, Massachusetts: Harvard University Press.

Lauer, Josh. 2017. Creditworthy: A History of Consumer Surveillance and Financial Identity in America. CUP Series on the History of U.S. Capitalism. Columbia University Press.

Mazzucato, Mariana. 2013. The Entrepreneurial State: Debunking Public vs. Private Sector Myths. 1st edition. London; New York: Anthem Press.

Newman, Abraham L. 2008. Protectors of Privacy: Regulating Personal Data in the Global Economy. Cornell University Press.

O'Mara, Margaret. 2019. The Code: Silicon Valley and the Remaking of America. New York: Penguin Press.

Rahman, K. Sabeel, and Kathleen Thelen. 2019. "The Rise of the Platform Business Model and the Transformation of Twenty-First-Century Capitalism." Politics & Society 47 (2): 177–204. https://doi.org/10.1177/0032329219838932.

Regan, Priscilla M. 1995. Legislating Privacy: Technology, Social Values, and Public Policy. Chapel Hill, NC: University of North Carolina Press.

Saxenian, AnnaLee. 1994. Regional Advantage: Culture and Competition in Silicon Valley and Route 128, With a New Preface by the Author. Cambridge, Mass.: Harvard University Press.

Thelen, Kathleen. 2018. "Regulating Uber: The Politics of the Platform Economy in Europe and the United States." Perspectives on Politics 16 (4): 938–53. https://doi.org/10.1017/S1537592718001081.

Whittaker, Meredith. 2021. "The Steep Cost of Capture." Interactions 28 (6): 50–55. https://doi.org/10.1145/3488666.

India's tryst with data privacy

Leon A. Morenas

India's privacy concerns center around the use of Aadhaar, a unique identification number assigned to resident of Indian. Aadhaar's uniqueness is ensured through biometric authentication and collection of verifiable socio-demographic data. It is a non-mandatory identification, but is required to open bank accounts, link provident funds, access welfare schemes and pay taxes online. To best understand the implications on privacy post-pandemic, it is important to understand the history of the project and how the pandemic offered the State yet another disaster to collect more granular personal data on its citizens.

History of Aadhaar

The Unique Identification Authority of India (UIDAI) was set up on 28 January 2009 to implement the Aadhaar flagship scheme. At this time enrollment was voluntary.

In order to avail of an Aadhaar card, people were expected to submit their demographic data (name, gender, date of birth, parent's or husband's name, residential address and any other information that the government prescribed) and three biometric markers (photographs, 10 fingerprints and both iris scans.) This information was then stored at UIDAI's Central Identities Data Repository (CIDR). At the time this was done absent a legal-frameworks elucidating the rights of the people enrolled or the duties of the state.

Slowly, Aadhaar was made compulsory for welfare programs and large swathes of the country's population were coerced into enrollment. For others, there was soft coercion, banks insisting on Aadhaar linkages, pensions and provident funds not being operable without them. Enrollment was boosted by incentive-based models for private agencies collecting the above information. Concerned citizens began approaching the courts to challenge the program in 2012 and between September 2013 and October 2015, the Supreme Court of India issued six interim orders to restrict the mandatory use of Aadhaar.

In 2016, almost seven years after the program was launched, the Indian government passed the Aadhaar Act or the Targeted Delivery of Financial and Other Subsidies, Benefits and Services Act. This marked the shift from the use of Aadhaar as a voluntary facility to a compulsory one.

"Data is the new oil," is an often-heard global mantra, and in India as one Twitter user put it, "Aadhaar is the drill to get it." UIDAI and its network has, since 2016, put in place a surveillance system linked across various government and private databases allowing for a 360-degree view of enrollees and their information.

On 24 August 2017, a nine-judge bench of the Supreme Court delivered a landmark verdict that placed privacy firmly in the center of democracy and integral to liberal human values of autonomy, dignity and freedom. This was in defiance of an argument made by the Attorney General for India two years prior that the Indian Constitution did not guarantee any fundamental right to privacy, and that any such judgement could be viewed as privileging the rights of the individual against the Indian State. But of course, what was left out is the wide range of private players who would also have access to Aadhaar data. The bench took cognizance of both points, and underscored the justiciability of privacy. It also ruled that that "private companies could not require citizens to provide their Aadhaar numbers for the provision of services."

This is in many ways a landmark judgement. But as some constitutional experts, argue the verdict "provides the *constitutional framework* within which ...cases are to be debated and

decided when they come before the courts... [The judgement] provides the foundation for a transformative civil rights jurisprudence. Or it could become only a rhetorical lodestar, a beautiful and ineffectual angel, beating in the void its luminous wings in vain."

Aadhaar and the Pandemic

The Indian State's response to the pandemic suggests that the State does in fact see the judgement as "a beautiful and ineffectual angel." India's COVID-19 Vaccine Intelligence Network (COWIN) was formally launched on 16th January 2021 as the platform for rolling out universal vaccine coverage. The functions of the platform included registration, appointment scheduling, identity verification, vaccination and vaccine certification. The data that was required for registering included name, mobile number, date of birth, gender and photo identification.

After receiving their first dose of the vaccine, some people noticed that a Unique Health ID (UHID) had been assigned to them on their vaccine certificates. No "consent" had been taken or information provided regarding the generation of the UHID. Those who had received their UHIDs were those that used Aadhaar as their photo identification. It is also unclear with whom that information resides and who all has access to it.

In <which month> a workshop entitled "Aadhaar 2.0: Ushering Ushering the Next Era of Digital Identity and Smart Governance," Ram Sevak Sharma, the first Director General of the UIDAI and now CEO of the National Health Authority, explained the issuance of UHIDs in the following manner, "You went for vaccination. You gave your Aadhaar to prove your identity. I gave a number. I gifted a number to you, a random number. Which law have I violated? Even, if I gifted that number to you without your permission. It's up to you to use that number or not to use that number, yaar. If I give a number to everybody in this hall and if you don't use that number, what crime have I committed?"

The Supreme Court judgement preventing private players from accessing Aadhaar information has privileged the State as a natural monopoly to collect citizen's data. The Abstract for the Interdisciplinary symposium on Rethinking Privacy after this Pandemic

absence of a Data Protection Bill has meant that the State now drafts policies like the "Draft India Data Accessibility & Use Policy 2022," to "radically transform India's ability to harness public sector data." The Bill sees data as a State asset that can be licenced, sold or shared with the private sector. This financialization of private data will in turn induce the State to collect more and more granular personal information for longer periods of time without a legal framework protecting the rights of India's citizens.

This paper is structured in two parts. The first part lays out the historical trajectory of the privacy story in India. (An concise outline of which, I have provided above.) The paper will expand on more recent events like the recent Criminal Procedure (Identification) Act 2022, where the bogey of crime is being used as the latest attempt to trample the privacy rights of Indian citizens.

The second part of the paper will be speculative. It presents two future scanios for India, one that draws from global best practices where companies and the State have attempted to value and preserve the right to privacy. The other more dystopian future that is proposed is one where the State tramples on the privacy of its citizens.

COVID-19 and an Everyday Account of Privacy

Manohar Kumar

A common way to understand COVID-19 is through the lens of public interest; anit-COVID response requires collaborative behaviour between different individuals and communities. It required everyone to contribute their fair share in ensuring the safety of others. By that virtue COVID-19 imposed a duty of fair play on every individual. One of the consequences of this duty was the trade-off that it entailed. The duty to ensure the safety of others required individuals to submit parts of their life to the scrutiny of the others, including the state. This way of framing the problem of COVID-19 relies on an existing philosophical framework of conflict of obligations in the face of a public interest problem. But this reading of COVID-19 leaves out the disruptive potential of COVID that can be termed as a transformative experience (Paul 2014) unable to be captured within existing rational categories of understanding. By framing COVID as a transformative experience we are able to capture its radically disruptive nature.

COVID demanded a fundamental reorganization of life through forced requirements of work from home. As more and more human activity got confined to homes, two domains of human activity , the home and the work became synonymous and continuous. The ease and the immersivity of the digital altered our understanding of space (all possible space was a workspace) and time (work and duties of care, household work can go on simultaneously). As differences between work and home got obliterated it challenged our conceptions and how we make meaning and organise our life in spaces. Modern everyday life requires a discontinuity between the private and the public with their different degrees, of what Thomas Nagel, calls concealment and exposure. The private is the zone of control, autonomy, experimentation, whereas the public is the zone of restraint and civility and learning to co-exist. Privacy enables individuals to formulate their ends in the manner they deem fit. Thus, the private and the public require different norms of behavior and action. COVID-19 obliterated this distinction by removing a form of privacy that prepared individuals for the (often arduous) task of representing themselves in the public spaces.

How should we understand the disruption caused by COVID? In this paper I argue that we require an everyday conception of privacy to make sense of the disruption caused by COVID. Arguments that frame privacy as a form of control or ownership of information, or as a form of restricted access fail to capture the disruptive nature of COVID that is radical existential uncertainty. Access or control based arguments frame the perspective of privacy based on the fact of an agent's control over information, or their privilege to restrict access to that information. At best they can respond to threats to privacy, under situations of health uncertainty like COVID, as a form of trade-off. Under this reading, privacy can be sacrificed in favour of the public good of health through a moral ordering where the fundamental right of privacy is sacrificed in favour of health (read life). This reading has its functions in terms of assigning normative weights to privacy and health and ensuring whether a proper trade-off has been achieved. But it has limited explanatory power in capturing the circumstances under which the choice between privacy and health are being framed.

I argue that trade-offs have a limited explanatory power precisely because they are framed within a conception of privacy that is representative of an order of things that is not radically disrupted. It depends on an 'all things considered' view where individuals are not faced with radical choices they face during emergencies. The private-public distinction is a form of

ordering of time and space in an everyday setting. It is a way of ordering our competing obligations and addressing requirements and demands that different spheres of life place on the individuals. In order to understand the disruption that COVID-19 causes we need to understand the private and public as ordinary categories that enable ordinary individuals to order their everyday life. In this regard, I rely on the work of Veena Das (2020) to understand the feelings of continuity, discontinuity, and disruption. The everyday and the ordinary because of its pervasiveness and ubiquity is elusive and evades description. But human beings rely, even without being conscious of it, on a conception of everyday to organise their life. This organisation enables them to make meaning and handle the disruptions of the everyday; the private can be a zone to retreat from the anxieties of the public and vice-versa. COVID-19 introduces a radical disruption, a form of extreme uncertainty, that cannot be captured within existing conceptions of everyday. COVID also created a norm gap; the existing norms were unsuitable, whereas the new norms were yet to be formed. The norm gap led to a gap between understanding and action and created a need to formulate a new balance between competing human interests. With COVID what is essentially disrupted is the everyday, the meanings attached to it, the norms, habits, actions, and the escapades built into it. Individuals are essentially forced to inhabit the same disrupted place and are asked to reorganise their lives without necessarily being certain about the tools through which they can make sense of the disruption and weave their life back.

An everyday conception of privacy is thus required to provide a rich understanding of both the context and the circumstances of the agent when making that choice. It also adequately captures the differential burdens, the ethical dilemmas, and the responses of differently placed agents who are comprehending the situation of uncertainty from their own situatedness. An everyday conception of privacy is also sensitive to the idea that circumstances and conditions of privacy are not the same for all individuals, and many individuals may lack the essential pre-conditions that make privacy possible. It also captures how individuals make sense of the disruption and formulate a response negotiating between their autonomy, control, and other competing interests.

References

Das, V. (2020). Textures of the Ordinary. In *Textures of the Ordinary*. Fordham University Press. Paul, L. A. (2014). *Transformative experience*. OUP Oxford

Risk Management in the Covid19 Pandemic and its Impact on the Rights to Privacy and Non-Discrimination

Danaja Fabcic Povse

In the covid-19 pandemic, authorities have relied upon scientific advice and risk management procedures to adopt public health measures to protect human lives. Public health risk assessment relies upon relevant data to answer questions such as who is likely to be affected, the likely exposure to the virus, which population is at risk, what is the societally acceptable level of risk etc.

Given the advanced technologies and data collecting practices used in public policy-making, legal scholarship has for a long time stressed the importance of using those tools in a manner compatible with the human rights to privacy and non-discrimination. I will discuss the impact on those rights in a public health context, analysing the risk-based measures e.g., lockdowns, tracking apps and digital certification, taken by authorities in the past two and a half years to limit the spread of covid-19. The analysis will contextualise the measure in the light of the case-law of the ECHR related to public health matters, such as the seminal 2011 judgment Kiyutin v. Russia, and the more recent covid litigation, to answer questions about suitability and proportionality of interference with privacy and non-discrimination.

Medical Privacy in the Wake of the 1889 ‚Russian Flu' Pandemic

Chris Zajner

The 1889 Russian (also called 'Asiatic') Flu epidemic can be described as an early pandemic. Prior to this period infectious diseases were limited in extent due relatively circumscribed human mobility. Yet, the development of extensive railroad networks during this period facilitated the previously unprecedented movement of goods and people around the world. It additionally propagated the process of shrinking the barriers between the countryside and major metropolises. While the current COVID-19 pandemic has resulted in lockdown measures nearly worldwide and has prompted widespread social, economic, and cultural disruptions, the Russian Flu was not accompanied by such drastic changes. I would like to argue that the reason this historic pandemic did not result in significant changes in societal discourse was a result of the scientific, medical, and technological mileau of the time. More specifically I will argue that the lack of a firm scientific understanding of the etiology of the infectious agent of 'influenza' hindered the ability of the public to formally recognize the reality and potential danger of the epidemic. The implications that this epidemic also had on the restrictions of individuals privacy in the longer term will also be investigated.

The 1889 Russian Flu pandemic has been estimated to have resulted in the death of over 1,000,000 people, to have spread to the majority of the humanly habitable globe, and to have infected between 300 and 900 million individuals. Regardless of this major toll the historical memory of this virus has been relatively forgotten and overshadowed by the 1919 Spanish Influenza. However, the Russian flu has recently been suggested to have been a coronavirus rather than influenza, and thus may serve as a closer cognate of the COVID-19 pandemic. Using accounts of the societal and medical response to the Russian Flu, as well as clinical case reports I intend to discuss the potential reasons for why this virus did not have a major effect on society at the time. My primary source will the broad ranging clinical and statistical information in Dr. Franklin Parsons synoptic report on the epidemic. I will also assess contemporary journal articles and published materials on the societal impact of the epidemic. How did trust in medical professionals, in the veracity of bacteriology, and in public health measures play a role in the trajectory of this pandemic.

In sum I will attempt to elucidate why this epidemic did not have a major effect on society at the time. Was it a result of the lack of medical or epidemiological ability to functionally counteract the virus? Was there a lack of public health organization to advocate for preventative measures? Was it a result of the relative disrepute of the medical profession at the time? Or discrepancies in the theoretical explanation of the spread of disease and lack of trust in holders of 'knowledge' ad statistical evidence? I will argue that all these played substantive roles in the relatively muted response to this pandemic. I will also argue that the different conceptual understanding of 'infectious illnesses' at this time highlight the way scientific and societal conceptions radically alter psychological responses to disease. In particular I will analyze the manner in which this epidemic was the beginning of the erosion of individuals privacy in the name of 'public health'. The growth of massive public service organizations and the stockpiling of statistical information were fundamental to this process.

Ultimately, the Russian flu brought about the growth of Influenza as a medical and scientific concept, and was the beginning of the process that saw individuals health care privacy and individuality eroded, for the sake of tackling common ailments. Yet, the major outbreaks in the

early 1890's – and their debilitating effects on society – were quickly forgotten from historical consciousness, much like the 1918-1919 Spanish Flu has been argued to have been. The main reasons for this phenomenon was a product of the delimited societal means to act upon the epidemic and control its spread. Influenza was not understood early on as due to a distinct etiological entity, as an infectious disease (as opposed to a miasmatic one), and most importantly was not practicably controllable through structured public health measures. As such it was not able to galvanize the public imagination for an extended period of time.

Neural Data: Not for Sale

Peter Zuk
Center for Bioethics, Harvard Medical School

Neural data derived from invasive and non-invasive recording techniques is increasingly utilized in healthcare and medical research. Despite this therapeutic utility, the prospect of expanded collection and use of neural data raises serious concerns, particularly in light of the looming proliferation of non-therapeutic consumer neurotechnologies envisioned by Neuralink's Elon Musk and other technoligarchs. Among these concerns are potential violations of brain privacy, mental integrity, and related neurorights. Rafael Yuste, Sara Goering, and other neurorights advocates therefore propose treating neural data as legally analogous to human organs, prohibiting its commercial transfer. I develop and assess one argument for this position: the objectification argument.

Adrian Walsh argues that the commercialization of a good tends to corrode recognition of its intrinsic value or that of related entities. The objectification argument applies this idea to commercialization of neural data. Non-therapeutic commercial uses of such data do not merely tend to corrode recognition of the intrinsic value of persons, the argument goes, but essentially involve a failure of such recognition. Thus, commercialization of neural data inappropriately objectifies and instrumentalizes the people whose data are used to profit.

Collection and use of neural data itself, for whatever purpose, also involves objectification of the individual it is about. That is, it involves viewing and treating them as a system that can be described and intervened upon mechanistically—a stance referred to by Iain Crinson as the "neuroscientific gaze." In medical practice and medical science, I claim, the neuroscientific gaze is permissible (and desirable) because essential reference is made to the person's own welfare and/or autonomy. (I here note, but set aside, complications introduced by the commercialization of medicine itself.) Thus, despite regarding the individual as a site of mechanistic intervention, the intervention also simultaneously regards them as an end qua person in virtue of attempting to benefit them and (except in extreme cases) seeking their informed consent. Essential reference is made to the good of the person intervened upon.

However, taking the neuroscientific gaze toward a person for purposes of selling a product is incompatible with valuing them as an end. Here we can distinguish two broad non-medical uses of neural data: use in selling itself (so-called "neuromarketing") and as itself an integral component of what is sold (as in direct sale of neural data, and potentially in sale of non-therapeutic consumer neurorecording devices—see below). In both cases, the neuroscientific gaze is taken in the absence of the concern for the person as an end that, in medical practice and medical research, render taking it permissible (and desirable). The person is viewed merely as a mechanistic system for intervention (and resulting profit), and thereby inappropriately objectified.

This, plausibly, is the kernel of truth in otherwise ambiguous concerns that novel neurotechnologies will result in dehumanization. But here we see that it is not the technologies as such that are objectionable, but instead their deployment for aims that make no essential reference to the good of those upon whom they intervene.

One might object at this stage that the objectification argument presupposes a controversial Kantian moral theory. But this is not so. To the contrary, proponents of other moral theories can endorse its claims as long as their theories allow for goods and bads (or rights and rights-

violations, or virtues and vices, etc.) that constitutively involve relations of a certain kind. And there are independent reasons for thinking that one's moral theory should do so.

I close by considering some options for fixing the scope of the objectification argument by considering precisely what is covered by the idea of commercialization of neural data. Most neurorights advocates have explicitly endorsed only a ban on the commercial transfer of neural data itself. The objectification argument identifies a plausible consideration in support of this position, and extends that consideration to the use of neural data to facilitate a commercial transfer ("neuromarketing") as well. Both of these uses of neural data involve the direct monetization of neural data. A proponent of the objectification argument might stop there. But it is worth asking whether the argument could plausibly be extended further—say, to the sale of non-therapeutic consumer neurorecording devices.

There is reason to believe it can. The sale of such a device seems still to involve taking the neuroscientific gaze for profit insofar as it amounts to conceiving of consumers as sites of profit in virtue of conceiving of them as sites of the neurorecording functions of the device. Even if one thinks this interpretation indecisive, the development of such a device for this purpose seems a more definitive case of taking the neuroscientific gaze for the aim of profit. Now, one might here point out, much as Walsh does in his treatment of the commercialization of medicine itself, that there are potential counterexamples afoot. An individual with altruistic motives might attempt to harness the market as a tool for the promotion of others' good. The degree of removal in this case, as compared to neuromarketing and the sale of neural data itself, seems to leave open that possibility. A proponent of the objectification argument might therefore here need to appeal to Walsh's distinction between commercialization of a good necessarily leading to a loss of recognition of intrinsic value, and its tending to corrode such recognition. It may be that while the stronger claim holds for neuromarketing and sale of neural data, only the weaker claim holds for sale of non-therapeutic consumer neurorecording devices.