Data Catalysis, Informational Violence, and the Denaturalisation of the Natural Person

Asad Rizvi*

I. The New Age of Discovery

Beneath the masts of the new conquistadors stretch the uncharted high seas of the digital where no state is able to claim jurisdiction. Here, hegemonic merchants circumnavigate between the Old World and the New to trade in bullion of unprecedented properties: data. Across this wild expanse, private actors have speared their flags of domination, governed only by commodious mercantile treaties. Laws that purport to protect local populations jostle powerlessly against an amassing tide of state-sanctioned yet private monolithic power, steered hypnotically by standard-bearers of a civilising faith to which dutiful observation is widely deemed a noble calling for humankind.[1]

Today, the dominant 'civilising missions' involve no priests. Cyberspace has appeared as the Earth's freshest *terra nullius* with a population undergoing an edification of its own kind. With the 'Death of God'[2] and the subsidence of religions as universal guiding truths during the latter half of the last century, market

* LL.B. Law (First Class Hons) and current LL.M. Human Rights Student at Birkbeck College, University of London. The author would like to express gratitude to Dr Oscar Guardiola-Rivera and Professor Bill Bowring, to whom this paper was originally submitted, and whose guidance was inspirational. The author is also deeply indebted to the *Cambridge Law Review* board for the opportunity, and to family members for patience and their proofreading of drafts.

1 Claims to new territorial sovereignty over lands deemed ungoverned by Europeans, succeeded only through the 'civilising missions' of the Churches, justified on grounds of natural reason. See John Witte and Richard C Martin (eds), *Sharing the Book: Religious Perspectives on the Rights and Wrongs of Proselytism* (Wipf and Stock 2008) 163.

2 Friedrich Wilhelm Nietzsche and Walter Arnold Kaufmann, *The Gay Science: With a Prelude in Rhymes and an Appendix of Songs* (1st edn, Vintage Books 1974) 167, 181.

efficiency has emerged as the primary metanarrative of power legitimation.[3] Just as some indigenous populations first received Christianity as a complement rather than a threat to their own belief systems,[4] online sociality has emerged as a virtual but independent prosthetic to the 'real',[5] whilst concealing mercantile functionalities under veneers of leisure.[6] Across the digital network, mechanisms of economic betterment prevail to steer happiness to such extent that humankind is in the process of handing over the helms of reasoned judgment to automated apparatuses of efficiency.[7] Human experience hence is distilled into quantified algorithmic input to improve shared understanding and to maximise revenue.[8]

[3] In 1984, Jean-François Lyotard presupposed the data revolution when he wrote that, through science, the contemporary age could be defined by "the incredulity toward metanarratives". "The decision makers", he wrote,

> attempt to manage these clouds of sociality according to input/output matrices, following a logic which implies that their elements are commensurable and that the whole is determinable. They allocate our lives for the growth of power. In matters of social justice and scientific truth alike, the legitimation of that power is based on its optimizing the system's performance—efficiency.

See Jean-François Lyotard, *The Postmodern Condition: A Report on Knowledge* (Geoff Bennington and Brian Massumi trs, University of Minnesota Press Minneapolis 1984) xxiv.

[4] Avelar relates that, in the 16th and 17th centuries, the Tupinambá people of present-day Brazil

> appeared malleable, accepting, and mimetic of the Portuguese values only, in a second moment, to look like they had forgotten everything and moved on to something else. In other words, what stunned the Portuguese was not the fact that there was a completely different set of beliefs in play. It was not the presence of a cosmogony contradictory with the Christian one. It was, rather, that the Tupinambá seemed to operate outside the Aristotelian logic of identity and non-contradiction altogether.

See Idelber Avelar, 'Amerindian Perspectivism and Non-Human Rights' (2013) 1 Alter/Nativas, 11–12.

[5] This can be epitomised by John Perry's *Declaration of the Independence of Cyberspace*, of 8 February 1996: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather." See Aron Mefford, 'Lex Informatica: Foundations of Law on the Internet' [1997] Indiana Journal of Global Legal Studies 211, 218.

[6] Adorno and Horkheimer's 1944 assertion that "[e]ntertainment is a prolongation of work under late capitalism" resonates ever more prevalently in the context of social media." See Theodor W Adorno and Max Horkheimer, 'Culture Industry: Enlightenment as Mass Deception' in *Dialectic of Enlightenment* (Blackwell Verso 1997) 109.

[7] For example, in 2017, Mark Zuckerberg laid out a manifesto for Facebook where AI fights for a "common understanding", identifies "risks" and decides which facts can be deemed credible or not. He talks of making leaps "from tribes to cities to nations" and reaching the next level of social infrastructure primarily through automation. See Mark Zuckerberg, 'Building Global Community' (6 February 2017) <https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10103508221158471/?pnref=story> accessed 21 May 2018.

[8] Rieder notes, "[s]oftware, again, is used to formalize and disambiguate notions of value and the resulting value signals are both directed to market participants and ranking algorithms. See Bernhard Rieder, 'Beyond Surveillance: How Do Markets and Algorithms "Think"?' (2017) 3 Le Foucaldien, 7.

As network and processing speeds increase with limitless storage possibilities, data technologies now are able to process previously inconceivable quantities of information to advance human knowledge and experience.

A paradox of the post-war era is that the globalisation of data technology has exploded in tandem with the most active period of human rights development. For Moyn, the term 'human rights' evokes romantic ideals of global utopia constructed upon individual dignity.[9] Yet he observes that the slipstream of market determinism has endorsed the simultaneous decline of social and economic rights, driving the betterment of individual wealth before that of individual well-being.[10]

The application of human rights has diversified since the Universal Declaration of Human Rights 1948 (UDHR), and so too have modes of power which have learned to circumvent its core principles. With new technologies proliferating modes of state oppression, many more subtle forms of violence remain unrecognisable within the original human rights framework, with latent potentialities for unprecedented consequences. Although 'traditional' weaponry remains in very much in use by states and their forces, more subtle disciplinary apparatuses—or *dispositifs*, as Foucault would call them[11]— are emerging through the processing of personal and bulk data in the private and public sphere. International legislators are not blind to these emerging forms of violence, but their ethereal properties make them uncontainable within traditional legal boundaries. This article seeks to address these leakages with a view to proposing a more comprehensive framework than is currently available. Must the jurisprudence of human and fundamental rights continue solely to restrain itself to the refrain of 'never again', or can it take another step forward with a more preventative objective of 'never shall it be'?

II. A Macro-Evolution of the Micro

A. Data catalysis

Numerous modes of data transformation exist as a result of the application of algorithmic processes upon user information, but since there is no common terminology for these disparate processes, this paper will refer to the collective paradigm as 'data catalysis'. Much like chemical catalysis,[12] algorithms increase the rate of forward and reverse transformations, and the energy threshold required is

[9] Samuel Moyn, *The Last Utopia: Human Rights In History* (Belknap Press of Harvard University Press 2012)

[10] ibid 35–36.

[11] Michel Foucault, *The History of Sexuality* (Vintage Books 1990) 96, 140.

[12] Antony Spiers and Derek Stebbens, *Chemistry by Concept* (Heinemann Educational Books 1973) 142; Donald A McQuarrie *et al, General Chemistry* (4th edn, Univ Science Books 2011) 663.

lowered, enabling large quantities to be processed at speed. In data catalysis, the 'catalyst' is algorithmic AI, and the 'substrate' can be thought of as the user's data. Automation accelerates processes of data transformation that otherwise would have to be untaken manually.

Within this umbrella term are contained numerous linked but distinct phenomena, including data mining,[13] personal data,[14] metadata,[15] big data,[16] artificial intelligence (AI),[17] behavioural targeting,[18] and algorithmic decision-making.[19] The processes commence with material acquisition and complete with transformation. Although there is a broad range of applications for data catalysis across multiple disciplines, it is the efficacy sought over our own species that simultaneously has rendered terms like 'metadata' and 'big data' to become both buzzwords and profanities in the media of recent years.

Clearly, the issue of most conspicuous controversy for data catalysis is that of privacy. This article would do little to add to the already voluminous body of

[13] The Oxford Dictionary defines 'data mining' as: "the practice of examining large pre-existing databases in order to generate new information." See Angus Stevenson (ed), *Oxford Dictionary of English* (3rd edn, OUP 2010).

[14] Article 4(1) 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.

See General Data Protection Regulation, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46' (2016) 59 Official Journal of the European Union (OJ) 294.

[15] The Oxford Dictionary defines 'metadata' as: "[a] set of data that describes and gives information about other data". See: Stevenson (n 13).

[16] The Oxford Dictionary defines 'big data' as: "[e]xtremely large data sets that may be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions". See ibid. A full definition is given in the next section.

[17] The Oxford Dictionary defines 'artificial intelligence' as: "[t]he theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages". See ibid.

[18] Blue Fountain Media define 'behavioural targeting' as:

> a technique used by online publishers and advertisers to increase the effectiveness of their campaigns through information collected on an individual's Web-browsing behavior, such as the pages they have visited or the searches they have made, to select which advertisements to display to that individual. The technique helps deliver online advertisements to the users who will be the most interested in them. Behavioral data can also be combined with other user information such as purchase history to create a more complete user profile.

See Blue Fountain Media, 'Behavioral Targeting – Glossary' (*Blue Fountain Media*, 29 October 2011) <https://www.bluefountainmedia.com/glossary/behavioral-targeting/> accessed 8 January 2018.

[19] The automated decision-making by computer algorithms, linked to AI.

literature on personal data and traditional surveillance. The issues surrounding metadata and big data, however, are not entirely detached, and must be understood together within the context of personal information.

Over the course of the post-war period, the Orwellian narrative has awakened the public to the diversity of personal intrusions that every new form of communication technology carries. Notwithstanding the ever-changing manner in which privacy violations take place, the principles established in Article 12 of the UDHR (which alludes to non-interference with an individual's privacy, family, home or correspondence) and Article 8 of the European Convention of Human Rights (ECHR) (right to respect for private and family life) are inescapable where the content of private information is intercepted, including those of proportionality against competing interests.[20] In Europe, the legal right to privacy has flowed with relatively healthy correlation to developments in information technology.[21] Rooted in Article 8 ECHR privacy rights, and the European Union (EU) Charter's derivative right to data protection,[22] personal data remains the remit of the individual.[23]

Conversely, federal laws in the United States of America (US) do not provide similar guarantees for the individual, favouring the interests of national

[20] Such as the limitations in Article 8(2), or where there is a 'reasonable expectation of privacy' as per *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22.

[21] In 1980, the OECD was quick to recognise issues of inter-jurisdictional data flow by setting out its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, a non-binding guidance. These principles were adopted by the Council of Europe a year later in Convention 108 to set down limitations in how data is handled whilst maintaining a consistent flow of data for the purposes of trade. The 1995 Data Protection Directive (DPD) served to ratify the objectives of Convention 108 at European Community level so as to ensure a harmonised protocol for both automated and non-automated data across both the public and private sectors. Although the Directive set out to protect individuals' Article 8 rights, it made no mention of human rights, instead focusing on the procedural duties of data controllers. In 2000, the Charter of Fundamental Rights of the European Union first established data protection as a right unto its own, thus consolidating the principles set out in the 1995 DPD and ECHR. The Charter did not come into force until 2009. See European Convention for the Protection of Human Rights and Fundamental Freedoms 1950; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 108 European Treaty Series (1981); Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data 1995; Charter of Fundamental Rights of the European Union 2000; Sian Rudgard, 'Origins and Historical Context of Data Protection Law' in Eduardo Ustaran and International Association of Privacy Professionals (eds), E*uropean Privacy: Law and Practice for Data Protection Professionals* (International Association of Privacy Professionals 2012) 6–17.

[22] *Charter of Fundamental Rights of the European Union.*

[23] *Copland v The United Kingdom* No. 62617/00 (European Court of Human Rights 4 March 2007).

security and law enforcement.[24] Where data protection exists for US citizens, it usually does not apply to foreign nationals.[25] In 2000, the EU Commission's *Safe Harbour* decision declared the exchange of data between the EU and US to be consistent with the provisions of the EU's 1995 Data Protection Directive, and that US data protection laws in the US sufficed to provide equivalent protection for Europeans.[26] Yet the *Safe Harbour* accord did not preclude government agencies in the US from indiscriminately accessing EU residents' personal data amidst the wave of post-9/11 emergency legislation.[27] These included a 2008 amendment to grant immunity to private firms that offered assistance to intelligence agencies,[28] thereby creating a corporate buffer for state surveillance. The National Security Agency (NSA) itself boasted "direct access" to the servers of nine major consumer companies—including Microsoft, Yahoo, Google, Facebook, and Apple—as part of its PRISM surveillance programme.[29]

Back across the ocean, the British Government Communication Headquarters' (GCHQ) Project Tempora programme placed interceptors on 200 of the underwater cables that came to shore, collecting 21 petrabytes of data per day[30], all of which was shared with the NSA and its 850,000 private contractors.[31] On account of the United Kingdom's (UK) advantageous geographic location between Europe and North America, GCHQ were able, by 2010, to intercept a quarter of the world's internet traffic,[32] making it arguably the most extensive and

[24] Policy Department C: Citizens' Rights and Constitutional Affairs, 'A Comparison between US and EU Data Protection Legislation for Law Enforcement Purposes' (European Parliament (Directorate General For Internal Policies) 2015) 7.

[25] ibid.

[26] *Commission Decision 2000/520/EC 2000* [2000] L 215/7 OJ.

[27] These include: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (2001) 107–56 (United States); These include: Homeland Security Act (2002) 107–296 (United States); Detainee Treatment Act (2005) 109–148 (United States); Military Commissions Act (2006) 109–366 (United States); Foreign Intelligence Surveillance Act of 1978 Amendments Act (2008) 110–261 (United States).

[28] *Foreign Intelligence Surveillance Act of 1978 Amendments Act (2008).*

[29] Paul Bernal, 'Data Gathering, Surveillance and Human Rights: Recasting the Debate' (2016) 1 Journal of Cyber Policy 243, 4.

[30] The equivalent of 30.5 million CD-ROMs per day: Tim Fisher, 'Terabytes, Gigabytes, & Petabytes: How Big Are They?' (Lifewire, 20 September 2017) <https://www.lifewire.com/terabytes-gigabytes-amp-petabytes-how-big-are-they-4125169> accessed 12 December 2017.

[31] Kadhim Shubber, 'A Simple Guide to GCHQ's Internet Surveillance Programme Tempora' (WIRED UK, 24 June 2013) <http://www.wired.co.uk/article/gchq-tempora-101> accessed 12 December 2017.

[32] GCHQ, 'Supporting Internet Operations' (GCHQ 2010) 3.

intrusive intelligence agency of the 'Five Eyes' group of nations comprising the US, UK, Canada, New Zealand, and Australia.[33]

B. 'This is just metadata'

The scale of the NSA's and GCHQ's surveillance programmes came to light in 2013 with the Edward Snowden leaks, revealing major flaws as a result of jurisdictional disparities, as well as new and unrecognised forms of surveillance.[34] The reassurance by Dianne Feinstein, chair of the Senate intelligence committee, that "this is just metadata"[35] did little to quell the fears of data experts who already understood its implications.[36] Although not as immediately invasive as phone-tapping, Bernal notes that metadata is more efficient for surveillance than content.[37] Snowden stated that GCHQ collected metadata from "every visible user on the Internet".[38] Despite the arduous and unreliable task of filtering high volumes of data, the complexity of collected metadata could reveal a plethora of personal details and relationships;[39] and as the former head of the CIA, General Michael Hayden, candidly stated, "we kill people based on metadata".[40] Although most citizens will not suffer assassination as a result of e-mail headers, the very existence and public knowledge of modern panoptic technologies, as Richards observes, has

[33] Ewen MacAskill et al, 'Mastering the Internet: How GCHQ Set out to Spy on the World Wide Web', *The Guardian* (21 June 2013) <http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet> accessed 13 December 2017.

[34] Bernal (n 29) 4–5.

[35] John Naughton, 'NSA Surveillance: Don't Underestimate the Extraordinary Power of Metadata', *The Guardian* (21 June 2013) <http://www.theguardian.com/technology/2013/jun/21/nsa-surveillance-metadata-content-obama> accessed 12 December 2017.

[36] Matt Blaze, 'Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)' (*WIRED*, 19 June 2013) <https://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again/> accessed 13 December 2017.

[37] Bernal (n 29) 6.

[38] Nigel Morris, 'Edward Snowden: GCHQ Collected Information from Every Visible User on the Internet' (The Independent, 25 September 2015) <http://www.independent.co.uk/news/uk/home-news/edward-snowden-gchq-collected-information-from-every-visible-user-on-the-internet-10517356.html> accessed 12 December 2017.

[39] Shubber (n 31).

[40] Johns Hopkins University, 'The Johns Hopkins Foreign Affairs Symposium Presents: The Price of Privacy: Re-Evaluating the NSA' (7 April 2014) <https://www.youtube.com/watch?v=kV2HD-M86XgI> accessed 12 December 2017.

a substantially disfiguring effect on power dynamics and threatens the effective functioning of democracy.[41]

The Snowden revelations caused an Austrian citizen, Maximillian Schrems, to take a case to European Court of Justice that, in 2014, struck down the entirety of the *Safe Harbour*[42] agreement for its inadequacy in safeguarding EU residents' rights against indiscriminate surveillance by US government agencies.[43] Citing the *Digital Rights Ireland*[44] case, the Court emphasised that the acquisition of information is enough to establish an interference of rights.[45]

In 2016, shortly after the Schrems decision, the EU finalised the General Data Protection Regulation 2016 (GDPR) that came into force in May 2018. The regulation constitutes the most comprehensive piece of data protection legislation seen globally to date, and sets out a number of developing rights including the right to be forgotten, the right to restrict processing, and the right to be informed.[46] Although, as van der Sloot reflects, these rights are constructed as fundamental rights that apply horizontally between private parties,[47] they originate from the right to privacy.[48] All such rights concern the individual, but leave exposed many other issues that emerge across the data catalysis paradigm.

III. Micro-Devolutions of the Macro

Big data's relationship to the individual is less immediate. Whilst there is no agreed definition of 'big data', a common conception is that which comprises the 'four Vs':[49] the collection of large *volumes* of data, from *various* sources, processed

41 Neil M Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934, 1951–1952.

42 *Commission Decision 2000/520/EC* (n 26).

43 Case C–362/14 *Maximilian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.

44 Case C–293/12 *Digital Rights Ireland and Seitlinger and Others* [2012] ECLI:EU:C:2014:238.

45 "To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference (judgment in *Digital Rights Ireland* and Others, C–293/12 and C–594/12, EU:C:2014:238, paragraph 33 and the case-law cited)." See *Maximilian Schrems v Data Protection Commissioner* (n 43) para 87.

46 *Regulation* (n 14).

47 Bart van der Sloot, 'Legal Fundamentalism: Is Data Protection Really A Fundamental Right?' in Ronald Leenes et al (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures*, vol 36 (Springer 2017) 6–7, 13.vol 36 (Springer 2017

48 ibid 5–6.

49 Bart van der Sloot et al (eds), *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016) 14; IBM, 'Infographic: The Four V's of Big Data | IBM Big Data & Analytics Hub' (*IBM Big Data and Analytics Hub*, no date) <http://www.ibmbigdatahub.com/infographic/four-vs-big-data> accessed 30 November 2017.

at high *velocity*, and checked for *veracity*.[50] Once bulk data has been acquired and processed it is used to create predictive crowd data, and applied through profiling.[51] Big data, as Oostveen points out, is far from a unitary phenomenon, but a set of processes that invoke separate legal issues at every stage.[52]

Before addressing the widening concerns on subsequent pages, it is important to point out that blanket condemnation of these new technologies might be premature as big data and AI have the capacity to substantially assist human rights. Professors McGregor and Walden have pointed out the value of data analysis in monitoring and discerning patterns in human rights abuses, in establishing the accountability of perpetrators, and even in identifying human bias and preventing discrimination.[53]

Notwithstanding these genuinely positive applications of big data, the threats the new technology can pose to human rights are far more cogent, and require swift and perceptive legal responses to ensure advances do not run amok. Whilst European data protection law is becoming ever more sophisticated in response to technological demands, the 'traditional' privacy framework leaves open ambiguities.

Whereas personal data acquired through surveillance practices would fall under privacy laws, anonymised data circumvents the same laws for lack of identifiability.[54] Where the GDPR considers identifiable personal data to be the property of natural persons, it detaches the user from her data after anonymisation, with the controller retaining rights over the database in intellectual property law.[55] Where private data surveillance seeks to ascertain individuals' details, big data primarily seeks out crowd trends whereupon it constructs predictions.[56] Whereas private data can be located on a single computer system, big data is dispersed across a network or multiple networks, its multi-nodal nature often storing information in numerous jurisdictions, exposing it to unconsented access. Whereas nodes of information can easily be linked together in traditional data sets, big data relationships are more voluminous and are complex to ascertain.[57] Although the

[50] Laux also proposes two more Vs: the legal *validity* of data in hand, and *volatility* of changes in the world that might affect its relevance. See Christian Laux, 'The Legal Aspects of Big Data' [2014] Swiss Analytics Magazine, 15–16.

[51] Sloot *et al* (n 49) 9.

[52] Manon Oostveen, 'Identifiability and the Applicability of Data Protection to Big Data' (2016) 6 International Data Privacy Law 299, 300–302.

[53] Bingham Centre for the Rule of Law, 'Artificial Intelligence, Big Data and the Rule of Law' (Event Report, The Law Society 9 October 2017) 4, 7.

[54] Oostveen (n 52) 306–307.

[55] Richard Kemp et al, 'Legal Rights in Data' (2011) 27 Computer Law & Security Review 139, 2.

[56] Oostveen (n 52) 301–302.

[57] Deepali Aggarwal, 'Difference between Traditional Data and Big Data' (Project Guru, 30 June 2016) <https://www.projectguru.in/publications/difference-traditional-data-big-data/> accessed 30 November 2017.

appropriation of personal data is clearly subject to transparency principles under data protection law, the use of that information once anonymised is less defined.

As the Snowden leaks revealed, not only are states able to evade their data protection duties behind the shield of private companies,[58] but non-state parties have also created a space where private actors wield a similar degree of influence and power over individuals' lives with scant accountability.[59] The Internet is the only mode of human communication that remains unregulated by a binding international treaty[60] in key with the neo-liberal fondness of informal and tractable forms of discretionary law.[61] Zalnieriute observes that, on account of the private stewardship on the net, companies have set out their own thresholds of human rights enforcement in accordance with their commercial goals.[62] The ensuing empirical effect on individuals is that of an unprecedented form of social contract without the need to establish formal state sovereignty. As Mejias analogises, the relationship of users to the digital network is reminiscent of colonialism, whereby colonial power imposed subjecthood without offering citizenship.[63] After the

[58] Another example is of the US telecommunication provider Verizon being ordered to hand over details of all calls to the NSA. See *In re application of the Federal Bureau of Investigation for an order requiring the production of tangible things from Verizon Business Network Services, Inc on behalf of MCI Communication Services, Inc d/b/a Verizon Business Services* No. BR 13-80 (United States Federal Foreign Intelligence Surveillance Court 25-4-13).

[59] To exemplify, Mark Zuckerberg's hearing at the Senate, not taken under oath, was marked by interactions of this sort:

> [SENATOR] FLAKE: …[D]o you believe that Russian and/or Chinese governments have harvested Facebook data and have detailed data sets on Facebook users? Has your forensic analysis shown you who else, other than Cambridge Analytica, downloaded this kind of data?
>
> ZUCKERBERG: Senator, we have kicked-off an investigation of every app that had access to a large amount of people's data before we locked down the platform in 2014. That's underway, I imagine we'll find some things, and we are committed to telling the people who were affected when we do. I don't think, sitting here today, that we have specific knowledge of—of other efforts by—by those nation-states. But, in general, we assume that a number of countries are trying to abuse our systems.

See Bloomberg Government, 'Transcript of Mark Zuckerberg's Senate Hearing', *Washington Post* (10 April 2018) <https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/> accessed 8 June 2018.

[60] Monika Zalnieriute, 'The Anatomy of Neoliberal Internet Governance: Queer Critical Political Economy Perspective' in Dianne Otto (ed), *Queering international law: possibilities, alliances, complicities, risks* (Routledge research in international law, Routledge 2018) 15.

[61] William E Scheuerman, 'Economic Globalization and the Rule of Law' (1999) 6 Constellations 3.

[62] Zalnieriute (n 60) 26.

[63] Ulises Ali Mejias, *Off the Network: Disrupting the Digital World* (Electronic Mediations Volume 41, University of Minnesota Press 2013) 8.

opaque processes of anonymisation, as discussed in the next section, subtle forms of violence begin to occur within the indeterminate zone of the digital.

IV. Into the Big Data Processing Plant

The procedures of big data are diverse and complex. To correctly assess the interplay between human rights law and big data, we must look at its processes rather than effects. Oostveen has identified a consolidated model to simplify its processes into three overarching phases—namely, acquisition, analysis and application[64]—that can assist us in identifying human rights issues at every stage.

A. Mining the Raw Materials

At the first stage is the *acquisition* of big data's raw materials.[65] These can be identifiable and anonymous data, as gathered through data mining, consensual data disclosure (such as through social media data), data sensors (such as global positioning system (GPS)), surveillance, and from the sale of data to third parties.[66] McDermott notes that, irrespective of whether activity is taking place in solitude, between users, or between users and above, surveillance is being conducted continually from the watchtowers of state or private institutions, whether by human or machine interception.[67] Data appropriation at this stage relates to traditional forms of raw and unprocessed monitoring, in multiple formats, of individuals in terms of their *natural* personhood. As such, standard Article 8 privacy rights apply, as does the fundamental right to data protection, and its subsidiary rights. Article 4(1) of the GDPR defines personal data as being "any information relating to an identified or *identifiable natural person*",[68] listing a number of identifiers such as name, online handles, location data, or other personal traits that are now familiar within human rights instruments.

B. Alchemic refinements

After the data is acquired, it must then be analysed.[69] It is at this stage that big data's new paradigms emerge. As big data is concerned with trends, data sets are assimilated and often anonymised.[70] On paper, anonymised data ought to fall

64 Oostveen (n 52) 306.
65 ibid 306–307.
66 ibid 307.
67 Yvonne McDermott, 'Conceptualising the Right to Data Protection in an Era of Big Data' (2017) 4 Big Data & Society, 4.
68 Emphasis added.
69 Oostveen (n 52) 307.
70 ibid 301.

below the threshold for data protection. What remains opaque is the process that follows anonymisation.

In 2006, Netflix announced a public contest to offer a prize for best film recommendation algorithm by releasing a data set containing 500,000 anonymised film recommendations.[71] Researchers Narayanan and Shmatikov revealed the 'leakiness' of this dataset by cross-correlating it against users' publicly available film ratings on the Internet Movie Database (IMDb) and were able to identify individual records and even ascertain political, religious and sexual preferences.[72]

When two or more anonymised datasets are combined, it is therefore possible to merge data to produce 'commingled data',[73] which too can compromise individual privacy.[74] The process could be likened to a notepad of tracing paper in which indistinct facial features are drawn on every page, but when overlaid with other pages, a clear identity can be ascertained. Data sources are growing by the day and include government, commercial, transactional, private, open-source, electoral and lifestyle, among other forms of datasets,[75] many of which are available to all as public or open data.[76] Given the relational nature of big data, information can also be gathered about a person from the data that is mined from others they know.[77] The technical possibility of irreversible anonymisation is widely refuted, opening up the risk of misuse by third parties.[78] Further concerns have been raised about AI systems choosing data sources by themselves, and creating metadata through their own analysis, for example facial recognition software being used to take guesses at a user's sexuality,[79] thereby taking liability for discriminatory analysis away from human actors.

Even where data is legally compliant, analysis can produce discriminatory information, unbeknownst to users. Data protection rights will apply to the new data, but traceability is difficult where companies do not follow principles of

[71] Kate Greene, 'The $1 Million Netflix Challenge' (*MIT Technology Review*, 6 October 2006) <https://www.technologyreview.com/s/406637/the-1-million-netflix-challenge/> accessed 5 September 2018.

[72] Arvind Narayanan and Vitaly Shmatikov, 'Robust De-Anonymization of Large Sparse Datasets (How to Break Anonymity of the Netflix Prize Dataset)' in (2008 IEEE Symposium on Security and Privacy, IEEE May 2008) 11.

[73] Kemp *et al* (n 55) 29–30.

[74] Oostveen (n 53) 307.

[75] Graham Smith, 'How To Build Geodemographics From Big Data' (CACI March 2016) 13.

[76] ibid 17; Great Britain and others, *Open Data White Paper: Unleashing the Potential.* (Stationery Office 2012) 8.

[77] McDermott (n 67) 4.

[78] Oostveen (n 52) 306.

[79] Bingham Centre for the Rule of Law (n 53) 5.

transparency.[80] For all its positive steps forward, the GDPR lays down no binding terms on commingled data, only paying it lip service in Recital 26 of the Preamble.[81] Its force applies to "identifiable natural persons", including pseudonymised data that can be re-identified.[82] It goes on to clarify, however, that data protection does not apply to anonymous information.[83] The legal personhood of the natural person, once de-identified, is dissolved within the digital space. Nature, by this jurisprudence, is contingent on identity. Therefore, when stripped of identity, a person is also stripped of natural personhood.

C. Into the turbines of power

Big data's third phase is *application*, wherein post-analysis data is treated as knowledge by which decisions are made.[84] A key concern in application is the re-purposing of data. Although anonymous groups are targeted, it is individuals who ultimately are affected.[85] For example, Thielman reports that personal medical information given to doctors might be anonymised before being sold, but then data-miners will commingle that information with other data sets, including public records, to create targeted advertising for pharmacies.[86] Of more prominent notoriety are the activities of marketing firms, such as the fallen Cambridge Analytica, who combined online quiz data, social media data, with polling data,

[80] Robert Madge, 'Five Loopholes in the GDPR' (MyData Journal, 27 August 2017) <https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm> accessed 11 December 2017.

[81] "The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person." See *Regulation* (n 14), Recital 26.

[82] Article 4(5) defines 'pseudonymisation' as:

> the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

See ibid.

[83] Including that used for statistical or research purposes. ibid, Recital 26.

[84] Oostveen (n 52) 307–308.

[85] ibid 307.

[86] Sam Thielman, 'Your Private Medical Data is for Sale—and It's Driving a Business Worth Billions', *The Guardian* (10 January 2017) <http://www.theguardian.com/technology/2017/jan/10/medical-data-multibillion-dollar-business-report-warns> accessed 6 December 2017.

to identify behaviours linked to voting habits, allowing them to create targeted advertising during election campaigns.[87]

Automated data application poses further problems with concerns being raised over the obfuscation of accountability for discrimination and unjust outcomes as a result of AI decisions.[88] Early manifestations of automated decision-making have yielded alarming outcomes, with Microsoft's Twitter-fed AI bot, Tay, famously tweeting that "Hitler did nothing wrong", and that feminists "should all die and burn in hell".[89] It is evident that such systems are still reliant upon quantitative input from the Internet over qualitative factors. Increasingly, big data will start to supplant actual human judgment in law enforcement, judicial and healthcare scenarios. Algorithmic technology is already in use in the USA through the COMPAS tool, which has proven to perpetuate discrimination within the criminal justice system.[90] Although Article 22 of the GDPR sets down a right "not to be subject to a decision based solely on automated processing", this right clearly will not be of great consequence retroactively, where that decision has had life-altering changes or even death.

V. Informational Decolonisation

A. Informational violence[91]

Can we argue that the *application* of data is a breach of privacy laws? It is hard to accept that millions of US citizens consensually parted with their lifestyle details whilst fully understanding the ramifications in political advertising that they would later see. Nor is it likely that patients would be content for information discussed in the privacy of the doctor's surgery to result in advertising relating to those very ailments. Whilst privacy-related legal protections are wide-ranging, the commercial and political *use* of that data is still left somewhat unaccounted for. If we think of a data protection breach as the intrusive observation of an individual's

[87] Cambridge Analytica, 'Cambridge Analytica – About Us' (30 September 2015) <https://cambridgeanalytica.org/about> accessed 18 February 2017.

[88] See Bingham Centre for the Rule of Law (n 53) 3; Mady Delvaux, 'Report with Recommendations to the Commission on Civil Law Rules on Robotics' (Committee on Legal Affairs – The European Parliament 27 January 2017).

[89] Alex Hern, 'Microsoft Scrambles to Limit PR Damage over Abusive AI Bot Tay', *The Guardian* (24 March 2016) <http://www.theguardian.com/technology/2016/mar/24/microsoft-scrambles-limit-pr-damage-over-abusive-ai-bot-tay> accessed 13 July 2018.

[90] Bingham Centre for the Rule of Law (n 53) 3.

[91] Portions of this section have been adapted from an unpublished LL.M. paper by the same author entitled: 'Oscillations of Identity, Violence and Sovereignty in Cyberspace'.

personal information by unwelcome eyes, behavioural targeting is the intrusive application of intelligence based on users' personal data.

Even the notion of autonomy expressed in Recital 7 of GDPR, whereby "[n]atural persons should have control of their own personal data" relies on the oxymoron of the natural person having access to the data. Digital denaturalisation, much like its physical counterpart, constitutes a loss of autonomy. While data protection is founded in the *appropriation* of data, the *transmission* of information, post-analysis, remains unaccounted for in law.

Although the technology and method are very different to subliminal advertising, now prohibited in most jurisdictions including the EU,[92] the upshot is not altogether different: a form of informational violence based on subtle psychological techniques of persuasion with the effect of distorting fair competition.

Informational violence can manifest in various forms. As Cybenko and others note, hacking techniques—such as Denial of Service attacks—interfere with computational processes and violate human *property*.[93] By contrast, informational violence impedes upon the cognitive processes of individuals. Informational violence thus constitutes a gradual and palpitating trespass into the solitary confine of the mind.

On the web, oscillations of threat and pleasure normalise what researchers at the University of Turin call "voluntary servitude"[94] that negate each other to create unconcern towards the machineries at play. Network leviathans prosper from this indifference. Each network comprises a vast anatomy of interconnected nodes that may apprehend practically limitless quantities of informational knowledge through AI, but continue to rely on humans to develop emotional intelligence. To this end, users provide the emotional system of the artificial humanoid of the web. Gerlitz and Helmond call this a "like economy", which now encompasses a range of emotions, from laughter, anger, sadness, surprise, and so forth.[95] From consensually acquired emotional intelligence, human weaknesses may thus be repurposed through automated transformation. Although, under Article 6 of the GDPR, repurposing is now prohibited, the bewildering array of privacy options

[92] An EEC directive of 1989 prohibited subliminal advertising. See Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by Law, Regulation or Administrative Action in Member States concerning the pursuit of television broadcasting activities 1989, Article 10(3).

[93] George Cybenko, Annarita Giani and Paul Thompson, 'Cognitive Hacking' in Marvin Zelkowitz (ed), *Advances in Computers*, vol 60 (1st edn, Academic Press 2003) 59.

[94] Alberto Romele, Francesco Gallino, Camilla Emmenegger and Daniele Gorgone, 'Panopticism is Not Enough: Social Media as Technologies of Voluntary Servitude' (2017) 15, 208–209.

[95] Carolin Gerlitz and Anne Helmond, 'The Like Economy: Social Buttons and the Data-Intensive Web' (2013) 15 New Media & Society 1349.

on every site is likely to produce what Schwab calls "consent fatigue",[96] whereby unconscionable policies will be accepted as the path of least resistance.[97]

Armed with emotive data, marketers and technology firms, from psychographic profiles, assign labels to individuals that rigidify algorithmic social categories, which as Mejias states, has the effect of foreclosing identities from variation.[98] Identity, for Deleuze, is formed through the resemblance of variations, yet within each variation are lesser variations that contradict similarity.[99] Big data's social labels do not presently account for such nuance. The violent biopolitical history of the 20th century already provides a lesson in social labelling. Yet these designations not only externally objectivise users, but as a 2016 study revealed, they have the dangerous capacity to influence self-perceptions based on trust in algorithmic reliability.[100]

Social networks further their habit-forming effects though techniques from the gambling industry, such as the scrolling gesture that replicates the reward-or-loss tenacity of slot machines.[101] Facebook's colour scheme also employs methods of visual science, whereby blue engenders trust and dependability, while its red notifications instigate urgency, strengthening its addictive qualities.[102] The site's co-founder Sean Parker acknowledges that the occasional dopamine hit of the liked photograph or post creates a "social validation feedback loop"[103] that encourages

[96] Pierre-Nicolas Schwab, '30 Days to Read Privacy Policies: Consent Fatigue Will Make GDPR Ineffective' (*Into the Minds*, 24 May 2018) <http://www.intotheminds.com/blog/en/30-days-to-read-privacy-policies-consent-fatigue-will-make-gdpr-ineffective/> accessed 6 June 2018.

[97] ibid; Richard H Thaler and Cass R Sunstein, Nudge (Yale University Press 2008) 35.

[98] Mejias (n 63) 83.

[99] Gilles Deleuze, *Difference and Repetition* (Columbia University Press 1994) xix.

[100] Christopher A Summers, Robert W Smith and Rebecca Walker Reezek, 'An Audience of One: Behaviorally Targeted Ads as Implied Social Labels' (2016) 43 Journal of Consumer Research 156, 171.

[101] Mattha Busby, 'Social Media Copies Gambling Methods "to Create Psychological Cravings"', *The Guardian* (8 May 2018) <http://www.theguardian.com/technology/2018/may/08/social-media-copies-gambling-methods-to-create-psychological-cravings> accessed 16 May 2018.

[102] Leo Widrich, 'Why Facebook Is Blue: The Science of Colors in Marketing' (*Social*, 25 April 2015) <https://blog.bufferapp.com/the-science-of-colors-in-marketing-why-is-facebook-blue> accessed 25 May 2018.

[103] Erica Pandey, 'Sean Parker: Facebook Was Designed to Exploit Human "Vulnerability"' (*Axios*, 9 November 2017) <https://www.axios.com/sean-parker-facebook-was-designed-to-exploit-human-vulnerability-1513306782-6d18fa32-5438-4e60-af71-13d126b58e41.html> accessed 25 May 2018.

daily activity. The social network thus promises reward in tandem with personally relevant novelty to produce a sense of belonging.[104]

In the current climate, much of the effects are well publicised, yet billions of users continue to engage on social media platforms regardless. In spite of the public controversies surrounding the practices of Cambridge Analytica and its parent company, the Strategic Communication Laboratories (SCL) Group,[105] Facebook boasted record revenues of $11.97 billion in the first quarter of 2018.[106] At the time of writing, investigations are being carried out into election meddling,[107] misuse of funds, illegal data appropriation and sharing,[108] but there remains no policy discussion relating to the post-processing relay of psychologically manipulative advertising itself. Thus far, a spate of dramatic 'tech trails' have taken place within the walls of legislatures, at the US Senate,[109] the EU Parliament,[110] and a UK Select Committee,[111] where testimony takes place without oath and with privilege against defamation. Online behavioural advertising is presided over by the self-regulatory Advertising Standards Authority, a private company,[112] whose rules remain founded in the collection of data and not delivery.[113]

[104] Björn Enzi, Moritz de Greek, Ulrike Prösch, Claus Tempelmann and Georg Northoff 'Is Our Self Nothing but Reward? Neuronal Overlap and Distinction between Reward and Personal Relevance and Its Relation to Human Personality' (2009) 4 PLoS ONE, 7.

[105] The Guardian, 'The Cambridge Analytica Files', *The Guardian* (17 March 2018) <https://www.theguardian.com/news/series/cambridge-analytica-files> accessed 8 June 2018.

[106] Facebook, Inc., 'Facebook Reports First Quarter 2018 Results' (25 April 2018).

[107] Jeremy White, 'Federal Trade Commission "Investigating Facebook after Cambridge Analytica Scandal"', *The Independent* (21 March 2018) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-cambridge-analytica-federal-trade-commission-ftc-investigation-privacy-rules-consent-decree-a8265906.html> accessed 8 June 2018.

[108] ICO, 'ICO Statement: Investigation into Data Analytics for Political Purposes' (*Information Commissioner's Office*, 3 May 2018) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/ico-statement-investigation-into-data-analytics-for-political-purposes/> accessed 8 June 2018.

[109] Bloomberg Government (n 59).

[110] Jennifer Rankin, 'Complaints that Zuckerberg "avoided Questions" at European Parliament', *The Guardian* (22 May 2018) <http://www.theguardian.com/technology/2018/may/22/no-repeat-of-data-scandal-vows-mark-zuckerberg-in-brussels-facebook> accessed 8 June 2018.

[111] Commons Select Committee, 'Alexander Nix to Appear Again before the Committee' (*UK Parliament*, 7 June 2018) <https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-nix-evidence-17-192/> accessed 8 June 2018.

[112] Advertising Standards Authority, 'About ASA and CAP' (*Advertising Standards Authority*, 2 March 2017) <http://www.asa.org.uk/about-asa-and-cap.html> accessed 8 June 2018.

[113] Advertising Standards Authority, 'Appendix 3 Online Behavioural Advertising' (*Advertising Standards Authority*, 21 November 2012) <http://www.asa.org.uk/type/non_broadcast/code_section/appendix-3.html> accessed 8 June 2018.

B. Informational self-determination

How then can human rights law respond to the informational violence of data technologies? And where lies the threshold of tolerance between innocuous advertising and psychological interference? In 1982, the German *Bundestag* legislated a population census that sparked controversy out of public fears that personal information could later be repurposed.[114] A year later, a class-action challenge was launched at the *Bundesverfassungsgericht* (the German Constitutional Court)[115] that lead to the creation of a principle called the 'right to informational self-determination to distinguish this problem from that of privacy.[116] As Rouvroy and Poullet stress, the right should not be mistaken for the right to maintain autonomy over one's own information,[117] a privacy issue now addressed by GDPR. Rather, the German court conceived informational self-determination as being the control of one's data as a means to ensure an autonomous existence as a citizen.[118] Hornung and Schnabel note that privacy and informational self-determination are interdependent but ultimately distinct legal matters.[119] In terms of the rights' application to modern data catalysis, it would be useful to prevent private entities and political parties from manipulating individuals based on their psychological weaknesses.

Although the freedoms of thought and conscience in Article 9 of the ECHR and Article 18 of the International Covenant on Civil and Political Rights (ICCPR) customarily are applied to religious issues, they also function to protect the manifestation of personal, political, philosophical, and moral beliefs,[120] a logical interlacement given that secular convictions neurologically occur in the same part of the brain as religious beliefs.[121] In the political context, a right to informational

[114] Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25 Computer Law & Security Review, 85–87.

[115] Volkszählungsurteil BVerfGE 65,1 Bundesverfassungsgericht, 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83.

[116] Hornung and Schnabel (n 114) 85–86.

[117] Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) 51.

[118] ibid 45–46; Hornung and Schnabel (n 114) 86.

[119] Hornung and Schnabel (n 114) 86.

[120] Jean-François Renucci, 'Article 9 of the European Convention On Human Rights: Freedom of Thought, Conscience and Religion' (Human Rights Files, Council of Europe 2005) 12–13.

[121] Neuroscientists from UCLA have proven that belief in religious and secular ideas occur in the ventromedial prefrontal cortex. See Allison Bond, 'Belief in the Brain' (*Scientific American*, 1 March 2010) <https://www.scientificamerican.com/article/belief-in-the-brain/> accessed 13 December 2017.

self-determination would constitute a hybridisation of Article 3 of the ECHR's Protocol, which requires that elections be held "under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature" with Article 9. The recent examples of psychological manipulation by shadowy forces during elections[122] will serve as a lesson learned from these early days of big data.

V. Relocating the Spatiality of Data Rights

The potential uses and misuses of data catalysis to human well-being and democracy are, at this early stage, as diverse as our own imaginations, and we can only guess where it will all go. How then might human rights be refurbished to respond reflexively to the overreaching of present and future technological phenomena?

The first area of development would be the enlargement of the right to data protection and associated rights, from being fundamental rights, to universal human rights. To account for the problem of territorial scope, the GDPR addresses jurisdiction comprehensively by expanding its reach to processors both in and outside of EU.[123] The problem, of course, is the practical reality of rogue organisations complying with these rules, and the enforceability of international law in third countries that do not provide adequate data protection. Therefore the direct and horizontal effect of fundamental rights of a EU Regulation is a considerable step forward for data subjects within the Union. Yet beyond terrain of the physical, data's ethereality becomes more apparent, revealing the material limits of state sovereignty.

Data's true terrain is, of course, cyberspace. Fletcher observes the disjuncture between the real and cyber as being based upon arbitrarily constructed yokes between the individual and socio-cultural artefacts.[124] If we are to dissolve such linkages and assess their empirical influence on social reality, their effects only manifest within the material and biological real. Wertheim draws a practical unification between the real and cyber by observing that the imaginary of

[122] Carole Cadwalladr, 'The Great British Brexit Robbery: How Our Democracy Was Hijacked', *The Observer* (7 May 2017) <http://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy> accessed 13 December 2017.

[123] Data protection applies where goods and services are offered to EU citizens, or where non-EU organisations monitoring data subjects within the EU. It also applies to processors that are established both in the EU and outside, irrespective of whether the processing occurs in the jurisdiction or not. Data transfers outside of the union must be to a third country deemed to offer adequate protection by the commission.

[124] Gordon Fletcher, 'Between Heaven and Charing Cross? Cyberspace as Urban Space' (*Spaceless*, 1995) <http://www.spaceless.com/papers/20.htm> accessed 20 November 2017.

cyberspace merely reiterates the Abrahamic reification of the celestial space as a foundation for law.[125] In the mediaeval imaginary space, there was regulation of the body *and* the soul, she writes. A critical factor at the time was that the universe was deemed finite, and could be quantified, albeit arbitrarily. Beneath the celestial strata of St Thomas Aquinas' jurisprudential taxonomy, lay the behavioural traits of all rational creatures that he ascribed as the natural law. With the tacit mandate of an omniscient Creator, these universal laws furnished the church and rulers with the building blocks of their own positive laws.

In the digital imaginary of the Internet, a different form of all-knowing entity exists in a new kind of cloud. Here, there is no jurisdiction without body. Much like Agamben's notion of the State of Exception as a legally sanctioned zone of lawlessness,[126] data catalyses are able to strip the user of political identity and autonomy—her *bios*. The user, then, is kettled into subgroups on the Internet whereupon they are bestialised into a commodified form of digital *zoē*,[127] where terrestrial laws are ineffectual. This ever-proliferating paradigm has snowballed in the name of the business efficacy. Algorithms, as Galloway insists, are firmly monolithic in their advancement of sanitised institutionalism,[128] yet by unlocking the secrets to human nature, data processes may be rationalised under the premise of collective betterment. Big data is the new natural law.

In practical terms, this suggests that laws on data need to be re-conceived as if cyberspace were real space. In 2016, the United Nations Human Rights Council passed a Resolution for "promotion, protection, and enjoyment of human rights on the Internet" emphasising "that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers".[129] Although a positive development, the Resolution was not binding and saw 14 countries vote against with 13 abstentions.[130] Clearly, for cyber law to be effective, the option for states to abstain creates a void where rules may be broken. As d'Amato states, the notion of consent in international law flies in the face of its purpose, as it gives states the prerogative not to adopt and ratify

[125] Margaret Wertheim, *The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet* (1st ed, WW Norton 1999) 18–43.

[126] Giorgio Agamben, 'The State of Exception as a Paradigm Of Government' in *State of Exception* (University of Chicago Press 2005) 1–31.

[127] Giorgio Agamben, 'The Politicalization of Life' in *Homo Sacer: Sovereign Power and Bare Life* (Stanford University Press 1998) 9–14.

[128] Alexander R Galloway, *The Interface Effect* (Polity 2012) 99.

[129] The Promotion, Protection and Enjoyment of Human Rights on the Internet A/HRC/32/L20 (United Nations 2016).

[130] Maëli Astruc, 'UN Human Rights Council Takes Actions On Internet Rights, Corporations' (*Intellectual Property Watch*, 14 July 2014) <https://www.ip-watch.org/2014/07/14/un-human-rights-council-adopts-resolutions-on-internet-corporate-responsibility/> accessed 15 December 2017.

legal principles that they find inconvenient.[131] Given the global impact of the Internet, localised norms do not suffice, allowing for private data firms and their funders to amass dangerous amounts of power around the world.[132]

The right to self-determination is one of the most ubiquitous human rights principles of all. Article 1 in both the ICCPR and the International Covenant on Economic, Social and Cultural Rights (ICESCR) state: "All peoples have the right of self-determination. By virtue of that right they freely determine their political status and freely pursue their economic and cultural development". After World War II, the right emerged as the primary tool to instigate decolonisation.[133] It since has been recognised by the international community as a peremptory norm binding upon all states.[134] Read outside the decolonialisation context, the words of Article 1 can be transposed to embrace the freedom to maintain one's political autonomy without interference, and freedom of economic and cultural choice. Informational self-determination as a universal peremptory norm, hence, will set a global standard for an even more politically, culturally and economically well-playing field, all of which are, of course, interlinked. It is clearly unrealistic to impose an outright ban on targeted advertising. A suitable threshold would therefore be to apply the principle where the thing advertised concerns the public at large.

Data processing is just one cogwheel in the techno-leviathan that is in dire need of regulation. The monoliths of the skyscraper and the black smartphone emerged as seemingly indestructible cultural institutions of the post-War capitalist era. Yet the manner in which both have been attacked signifies an unforeseen defencelessness within the neoliberal machine wherein any party with resources has been able to meddle.

The non-territorial ethereality of data is ample foundation for establishing international checks and balances, such as a World Court of Human Rights (as suggested by Nowak[135]) and an international convention that imposes binding

[131] Anthony d'Amato, 'Is International Law Really Law?' (1984) 79 Northwestern University Law Review 1293, 1309.

[132] Jack Lewis, 'Cambridge Analytica Endangers Global Democracy, and It Must Be Stopped', *The Diamondback* (20 November 2017) <http://www.dbknews.com/2017/11/21/cambridge-analytica-endangers-global-democracy-and-it-must-be-stopped/> accessed 14 December 2017.

[133] Although presented under the pretext of democracy, the post-War decolonial drive was founded by the US desire to break up the European stronghold of the south during the Cold War and to strengthen pro-capitalist numbers at the UN. See Leslie James and Elisabeth Leake (eds), *Decolonization and the Cold War: Negotiating Independence* (New approaches to International History, Bloomsbury 2015) 1–2.

[134] Responsibility of States for Internationally Wrongful Acts A/56/49(Vol I)/Corr4 (United Nations 2001).

[135] Manfred Nowak, 'The Need for a World Court of Human Rights' (2007) 7 Human Rights Law Review, 251–259.

human rights obligations on private corporations (as proposed in the Lima Declaration[136]). All such propositions are objects of a study unto their own, but notwithstanding other innumerable imperatives for such normative legal developments, data law itself is a pervading argument in their favour.

VI. Conclusion

In evolutionary terms, the Internet is the Earth's youngest wilderness. To contemporary powers it is a virgin territory where those who control its quarries may flourish under their own stipulations. Whilst the wanton *excavation* of its resources is seeing a steady sharpening of supervision by international common sense, the *exploitation* of those resources remains a prerogative in which highest bidders may luxuriate. Through efficient tools of mechanised processing, 'stock' is intermingled and bestialised through collective attributes, beyond law's grasp. In this indeterminate zone of *terra nullius*, individual personhood, in a denaturalised state of spectrality, is put to work in data's industrial complex, alienating the final material production from the natural human resources whence it came.[137] The final output, then, is used to automate new forms of natural law employed to further subjugate the very same populace.

Much like the civilising missions in the Age of Discovery, the maladies of data's informational violence will only be felt long after being diagnosed. The mutually beneficial privity of contract between data processors ensures that data's unseen processes evade human rights jurisdiction. International instruments and domestic law, hence, must reimagine cyberspace as the proximity of real territory, much like the seas and air, so as to prevent unprecedented abuses from these juridical voids. As Fanon wrote, during the process of decolonisation, the indigenous population were "discerned only as an indistinct mass".[138] We all are the indigenous population of cyberspace. A process of decolonisation has begun, but it still has much of a way to go before the mass once again are recognised as constituents of reality.

[136] Worldwide Movement for Human Rights (FIDH, 'Lima Declaration on Human Rights and Business' (2012) 1–6.

[137] Of alienation, Karl Marx wrote:

> The alienation of the worker in his product means not only that his labour becomes an object, an external existence, but that it exists *outside him*, independently, as something alien to him, and that it becomes a power on its own confronting him; it means that the life which he has conferred on the object confronts him as something hostile and alien.

See Karl Marx, *Economic and Philosophic Manuscripts of 1844* (Dover Publications 2007) 67–83.

[138] Frantz Fanon, *The Wretched of the Earth* (Constance Farrington tr, Penguin Books 2001) 34.