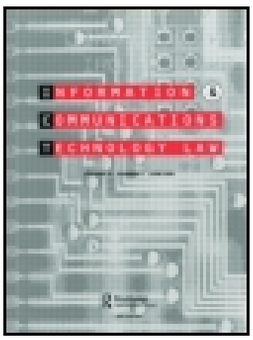

Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/cict20

Human digital thought clones: the *Holy Grail* of artificial intelligence for big data

Jon Truby & Rafael Brown

To cite this article: Jon Truby & Rafael Brown (2020): Human digital thought clones: the *Holy Grail* of artificial intelligence for big data, Information & Communications Technology Law, DOI: 10.1080/13600834.2020.1850174

To link to this article: https://doi.org/10.1080/13600834.2020.1850174

Published online: 01 Dec 2020.

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW
https://doi.org/10.1080/13600834.2020.1850174

Routledge
Taylor & Francis Group

Human digital thought clones: the *Holy Grail* of artificial intelligence for big data

Jon Truby and Rafael Brown

Centre for Law and Development, College of Law, Qatar University, Doha, Qatar

ABSTRACT

This article explores the legal and ethical implications of big data's pursuit of human 'digital thought clones'. It identifies various types of digital clones that have been developed and demonstrates how the pursuit of more accurate personalised consumer data for micro-targeting leads to the evolution of digital thought clones. The article explains the business case for digital thought clones and how this is the commercial Holy Grail for profit-seeking big data and advertisers, who have commoditised predictions of digital behaviour data. Given big data's industrial-scale data mining and relentless commercialisation of all types of human data, this article identifies some types of protections but argues that more jurisdictions urgently need to enact legislation similar to the General Data Protection Regulation in Europe to protect people against unscrupulous and harmful uses of their data and the unauthorised development and use of digital thought clones.

Keywords

Digital thought clone; digital clone; artificial intelligence; micro-targeting; human digital twins; algorithmic pricing

1. Introduction

How would you feel if a company developed a 'digital thought clone' of you, representing everything known about you, in order to predict and manipulate your choices in real time by using your own data against you for its profit? This would be your digital twin, made by constantly collecting your intimate personal data in real time even when you are asleep.

Given their commercial value, it is possible that every human has, or will have, a digital thought clone replicating all their known digital data at an industrial scale from data shared through free apps, social media accounts, gadgets, mobile phones, GPS tracking, monitored online and offline behaviour and activities, and public records. A digital thought clone, evolved from previous types of digital clones, goes beyond predictive analysis. It is a personalised digital twin comprising a replica of all known data and behaviour on a specific living person, recording their choices, preferences, behavioural trends, and decision-making processes. Artificial intelligence (AI) algorithms test strategies in real time, and predict, influence, or manipulate a person's consumer or online decisions. This is the ultimate advertising tool, as it is the closest representation a company would have of a living person's thoughts. It also enables companies to try to sell products and services at

CONTACT Jon Truby jon.truby@qu.edu.qa

the most effective time premium price, to influence a user's voting intentions, or to use intimate details of their personal digital life to decide whether their bank should grant them a loan. Digital thought clones tracking each user's every move can record who a person is meeting, who their friends are, what they talk about, what they are spending, and what they are reading.

Our willingness to trade personal data for the free and convenient use of technology, has enabled data miners to commercialise these data for use in predictive technologies, with increasing sophistication and relentless exploitation. Zuboff called this exchange of free services for data, enabling the detailed monitoring of behaviour, as 'surveillance capitalism'.[1] It is unimaginable that people would knowingly agree to any company collecting such levels of data on them, and would then allow those data to be used in such intrusive and personal ways that are already being deployed by big data and AI companies.

A digital thought clone is not only extremely dangerous for a person's privacy but is also potentially detrimental to their interests and ability to choose. US National Security Advisor Robert O'Brien warned that 'If you get all the information on a person and then you get their genome, and you marry those two things up … that is an incredible amount of power,' that could be used to 'micro-target' people and even to 'exploit their hopes and their fears'.[2]

The use of deepfakes[3] has made headlines in both entertainment and politics, and their potential dangers for creating misinformation and confusion have been noted.[4] Whereas the more entertaining type of visual and audio digital clones are well known, digital clones come in different types, all of which pose ethical, philosophical, and legal questions that need to be addressed.

This article discusses the legal and ethical issues raised by digital cloning and digital thought clones, and the need to re-conceptualise current theoretical notions on data privacy. Section 2 of the article provides a necessary definitional context for the different types of digital clones. This section categorises digital clones into audio-visual, memory, personality, and consumer behaviour cloning. It explains how such advancements have led to a risky path of normalising the purposeful creation of a digital thought clone for each natural person, or an individualised digital twin.

Section 3 argues that misaligned legal protections may be driven by theoretical concepts of data privacy that do not meet the realities of big data and AI. The section examines prevailing theoretical concepts of data privacy, such as the public/private dichotomy, and Nissenbaum's contextual integrity theory of data privacy.[5] It argues that the above theoretical views of privacy fall short when applied to AI and digital thought clones

[1] S Zuboff, 'You are now remotely controlled' *New York Times* (New York 20 January 2020) <https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html> accessed 11 February 2020.

[2] 'US warns Boris Johnson over Huawei risks to UK citizens' secrets' *Financial Times* (New York, 24 December 2019) <https://www.ft.com/content/686bfaf2-25d7-11ea-9a4f-963f0ec7e134> accessed 23 October 2020.

[3] A deepfake is the use of AI to 'merge, combine, replace and superimpose' audio, video, and images to create what seems an authentic audio and video. Marie-Helen Maras and Alex Alexandrou, 'Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos' (2019) 23 IJEP 255–62.

[4] S Cole, 'Deepfake of Boris Johnson Wants to Warn You About Deepfakes' *Motherboard Tech by Vice* (London, 13 November 2019) <https://www.vice.com/en_uk/article/8xwjkp/deepfake-of-boris-johnson-wants-to-warn-you-about-deepfakes> accessed 8 January 2020. (stating that '[t]he last thing any election cycle needs in the age of rampant misinformation is deepfake videos of candidates saying things they've never said').

[5] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 WLR 119.

that require the pervasive and continuous use of a person's data in both public and private spheres of overlapping contexts. The article argues that the legal protection of personal data can only work under a human-centred theory of data privacy.

Section 4 examines the various legal issues that digital cloning poses, including data privacy, informed consent, and laws against discrimination that may encourage behaviour cloning, copyright, and the right to publicity. It explains how the law seeks to protect people against the misuse of their data and identifies cases where the law absurdly encourages businesses to develop more personalised human digital twins.

Section 5 discusses the ethical questions raised by the creation of digital clones. It first conducts a general discussion of the ethical and moral objections raised by digital cloning in comparison to biological cloning.

Section 6 examines specific potential ethical issues raised by digital cloning, including consent and privacy, digital immortality, and the potential status of digital clones as people. It explains that the creation of a digital thought clone poses the immediate and most challenging questions to our existing notions of law and ethics. The article identifies the protections available in some jurisdictions against some of the risks of digital thought clones, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act of 2018 (CCSP). It then discusses the various legal and ethical issues raised by digital cloning and highlights the urgent need for stringent domestic regulations to protect citizens against the unauthorised development of digital thought clones and the associated risks of misuse.

2. Types of digital clones

The term 'digital cloning' has been used interchangeably to broadly cover several different types of AI algorithmic data and process replication. This section details the different types of digital cloning in order to distinguish the article's novel identification of digital 'thought cloning', which is emerging and evolving from the other types of digital cloning that have been identified. The discussion on the various types of digital cloning is a necessary precursor for the discussion on the ethical and legal issues that digital cloning raises in its various forms.

2.1. Audio and visual (AV) cloning

'Digital cloning' refers to the digital manipulation of images, audio, or videos. However, a more accurate term would be audio-visual or AV cloning. The term 'digital cloning' is used in this article to refer to all types of digital cloning, including AV cloning.

In AV cloning, the creation of a cloned digital version of the digital or non-digital original can be used, for example, to create a fake image, an avatar, or a fake video or audio of a person that cannot be easily differentiated from the real person it is purported to represent. AI can manipulate previous sound or video recordings of a person to create a 'deepfake'[6] version, which appears to be the person it represents. For example, the

[6]Luciano Floridi, 'Artificial Intelligence, Deepfakes and a Future of Ectypes' (2018) 31 PT 317–321.

previous video footage of both Facebook founder Mark Zuckerberg and former US President Barack Obama, have each been manipulated using AI software to produce doctored deepfake versions of the videos that seem authentic to human viewers.[7] AI software companies are developing and perfecting such technology for media editing and entertainment. The technology company Baidu demonstrated its ability to clone human voices by inputting as little as 3.7 s of sound clips.[8] These are often indistinguishable from authentic voices and have been used to defraud people out of money. An employee was once tricked into transferring GBP 200,000 by a deepfake impersonating his boss, instructing him to transfer the money.[9]

Users give access to their phones, computers, and TV microphones to technology companies in exchange for free convenient services. Major technology firms have listened to and recorded human conversations and have allowed AI to analyse those conversations to learn from them.[10] If the data were hacked or misused, it would be possible to create an AI voice clone of virtually any phone user on the planet.

2.2. Memory and personality: mindcloning

Another type of digital clone is the mindclone, which is essentially a digital copy of a person's mind.[11] Companies have collated digital data and behavioural and decision-making patterns for particular humans in order to make their digital versions. This allows relatives to continue interacting with an AI version of a person after their death. Using nanotechnology, companies are also trying to build a person within a physical robot, built to resemble the deceased human's behaviour, decision-making, and body movements. It is also possible for a robot to sound like a person using voice replication software.

A digital clone is created from 'mindfiles' that comprise the digitised version of the collective thoughts, recollections, feelings, beliefs, attitudes, preferences, and values of a person as processed by AI software called mindware.[12]

A mindclone of her deceased spouse, for example, was created by Martine Rothblatt, founder of the Terasem Movement, and the mindware was embedded in a robot replica called Bina48.[13] The Terasem Movement has already created thousands[14] of mindclones

[7]'A deepfake video of Mark Zuckerberg presents a new challenge for Facebook' *CNN* (New York 12 June 2019) <https://edition.cnn.com/2019/06/11/tech/zuckerberg-deepfake/index.html> accessed 26 October 2020.

[8]Sercan Arik and others, 'Neural Voice Cloning with a Few Samples' (32nd Conference on Neural Information Processing Systems, 2018) <https://arxiv.org/pdf/1802.06006.pdf> accessed 26 October 2020.

[9]'UK energy boss conned out of £200,000 in 'deep fake' fraud' *City AM* (London 6 October 2019) <https://www.cityam.com/uk-energy-boss-conned-out-of-200000-in-deep-fake-fraud/> accessed 26 October 2020.

[10]'Yes, tech companies may listen when you talk to your virtual assistant. Here's why that's not likely to stop' *CNN Business* (New York 19 August 2019) <https://edition.cnn.com/2019/08/19/tech/siri-alexa-people-listening/index.html> accessed 26 October 2020.

[11]Iegor Bakhariev, 'Digital Cloning – A Sci-Fi Dream or a Legal Nightmare?' *Inside Scandinavian Business* (Malmo 20 September 2019) <https://www.insidescandinavianbusiness.com/article.php?id=472> accessed 17 November 2019; Ichiro Fukumi, *Mind Replica (Mindclone) – A Means for Keeping Consciousness/Mind Permanently (Perspectives for Post-Singularity Age)* (FK Press, 2019); Martine Rothblatt, *Virtually Human: The Promise – and the Peril – of Digital Immortality* (St. Martin's Press, 2014); Tanya Lewis, 'The Singularity Is Near: Mind Uploading by 2045?' *Livescience* (New York 17 June 2013) <https://www.livescience.com/37499-immortality-by-2045-conference.html> (accessed 6 January 2020).

[12]Bakhariev (n 9).

[13]Natalie O'Neill, 'Companies want to Replicate your Dead Loved Ones with Robot Clones' *Motherboard Tech by Vice* (London 16 March 2016) <www.vice.com/en_us/article/pgkgby/companies-want-to-replicate-your-loved-ones-with-robot-clones> accessed 30 September 2019.

[14]At least 56,000 people have shared information with Terasem Movement to create mindclones.

for people who share their information to create mindfiles, with the aim of creating replica robots of deceased relatives.[15] While the Terasem Movement's mindclones like Bina48 are still socially awkward, they aim to make them ready for commercialisation in the next 10–20 years.[16]

The Terasem Movement is not the only company engaged in this emerging field of AI digital cloning. Google filed for a patent on a cloud-based robot personality that could replicate specific human personality traits.[17] The technology can be used to replicate the personality of a deceased person or celebrity and can be transferred across robot platforms.[18]

2.3. Consumer behaviour cloning

Marketing companies have long coveted the ability to predict consumer choices. The process of 'cloning your best customer' has been carried out for decades through profiling or 'clustering' customers based on demographics. Publicly available data sources such as census data, personal addresses, and lifestyle descriptors can be accessed to categorise consumers into clusters. Marketing companies were able to categorise groups such as 'baby boomers' and 'yuppies' to predict consumer choices, although without additional data, this risked creating only a cliché. More reliable consumer profiling can be developed through additional factors such as historic transaction data (showing income levels and spending) and customer attitudes through surveys.

Algorithmic software was developed with increasing levels of accuracy, as more data sources were added to profile consumers and predict their choices. Other factors that would create higher levels of predictive accuracy can now be rapidly accessed and analysed by AI software, including statistics on web search requests, data in open databases, and web reports. The AI analysis of searches and online purchase histories, combined with social media campaign results and existing public data, allows marketing companies to predict consumer trends. The accuracy has improved over time, but is still largely based on the statistical profiling of customers, which cannot entirely predict individualised choices. The user profile is built using 'explicit' user profiling by collating data entered by the user such as on questionnaires online and 'implicit' user profiling based on a user's digital interactions and history.[19]

The predictable evolution in digital cloning is to combine the various types of digital clones into one comprehensive digital clone. Such a digital clone would combine the attributes of the mindclone, and the AV and consumer behaviour clones into a single digital clone. Before this, however, there seems to be another category of a digital clone that can come from combining the attributes of consumer behaviour clones and mindclones with individualised digital data, to create a digital thought clone.

[15]Natalie O'Neill, 'Companies Want to Replicate Your Dead Loved ones with Robot Clones' *Motherboard Tech by Vice* (London 16 March 2016) <www.vice.com/en_us/article/pgkgby/companies-want-to-replicate-your-loved-ones-with-robot-clones> accessed 30 September 2019.
[16]O'Neill (n 14)
[17]ibid.
[18]ibid.
[19]Unfold Labs, 'AI Driven Personalization' *Medium* (San Diego11 June 2019) <https://medium.com/@Unfoldlabs/ai-driven-personalization-6dc9c47c1418> accessed 23 September 2020.

2.4. Digital thought cloning

Whereas consumer behaviour cloning seeks to create a profile of an ideal consumer based on a combination of different 'ideal' consumer data, digital thought cloning involves the creation of a digital clone that represents each individual consumer, or a digital twin.

Improving accuracy in predicting consumer trends involves collating as much data as possible on a specific human consumer. The ultimate goal is the creation of a digital clone involving a person's data combined with his/her previous consumer choices and decision-making patterns gauged through tracking data and analysis software. The concept of 'consumer behaviour cloning' applies to a category of human behaviour prediction based on probabilities. However, advancing this with the idea of cloning a particular person's decision-making using their individualised data, creates a clone specific to that person. This has numerous utilities, which makes it both highly valuable and extremely versatile.

Collating such data to create a digital thought clone would allow companies to predict a specific human consumer's choices to a high level of accuracy, rather than categorising the consumer into a profile.[20] Marketers can modify their advertising or sales techniques using AI to target specific customers with a higher probability of success rather than a cluster of customers at random. Online tracking cookies allow the tracking of consumer behaviour online, such as the type of product or service that a person searches for, how long they search for it, what search engines they use, which shopping or search comparison sites they trust, and how long they compare prices before making a decision. This can be combined with the analysis of existing records – both online and offline – including not only standard profiling data such as age, gender, marital status, race, financial data, spending habits, census, and credit cheques, and also specific collated data including, for example, a person's Internet search histories, social media contributions (e.g. likes, followed pages, comments, places visited, etc.), political views gauged from online readership and interaction, and any searchable online information such as news and location history from their phone.

Kosinski et al. explained how digital information can be used to predict a user's profile with great accuracy.[21] Figure 1[22] demonstrates the alarmingly high accuracy with which users' sensitive personal data can be discerned from a mere analysis of their likes on Facebook.[23] They identified that website browsing logs alone can estimate users' age, gender, education level, profession, and personality with high levels of accuracy.[24] Facebook's loyalty prediction can predict when a user is about to switch brands.[25] It can also predict how people feel, and pinpoint and match a user's emotional phase with an appropriate ad that can maximise potential sales.[26]

[20]John Naughton, 'The Goal is to Automate us': Welcome to the age of Surveillance Capitalism' *The Guardian* (London 20 January 2011) <https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook> accessed 11 February 2020. ('It works by providing free services that billions of people cheerfully use, enabling the providers of those services to monitor the behaviour of those users in astonishing detail – often without their explicit consent').

[21]M Kosinski, D Stillwell, and Graepel T, 'Private Traits and Attributes are Predictable from Digital Records of Human Behavior' (2013) 110 PNASUSA 5802.

[22]Kosinski (n 21).

[23]ibid.

[24]City AM (n 8).

[25]Zuboff (n 1).

[26]ibid.

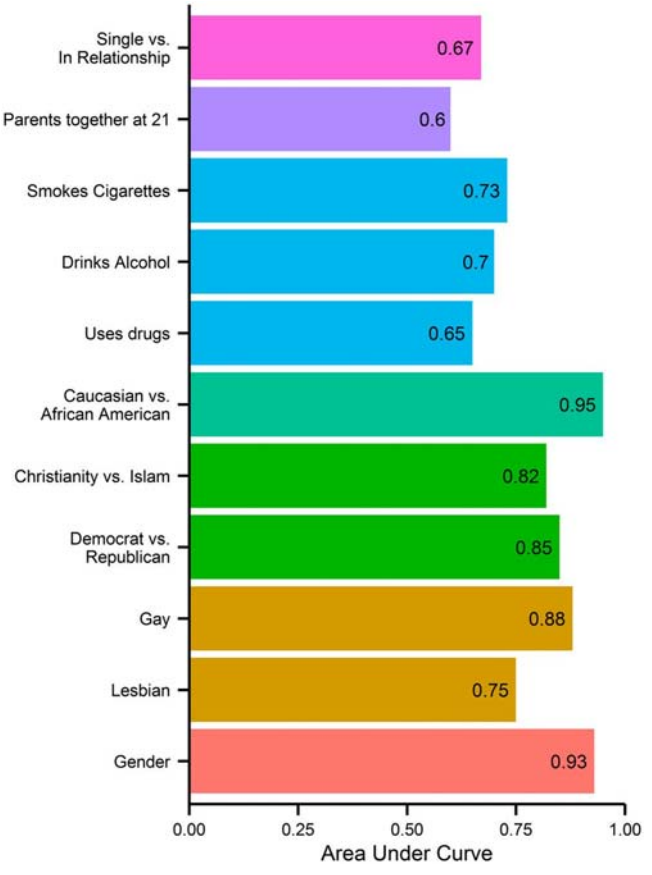

Figure 1. Private traits and attributes are predictable from digital records of human behaviour.

Apps often request access to a person's phone contacts; this helps an AI-driven algorithm understand the user's social group in addition to their social media presence.[27] Kerr and Earle explained that '[s]ome loan companies, for example, are beginning to use algorithms to determine interest rates for clients with little to no credit history, and to decide who is at high risk for default. Thousands of indicators are analysed, ranging from the presence of financially secure friends on Facebook to time spent on websites and apps installed on various data devices'.[28] That was in 2014, and the technology has evolved rapidly since then.[29]

Understanding the social group and acquiring information on the location history can allow predictive AI technology to determine, for example, whether one spouse in a married couple is sleeping outside of their usual sleeping place[30] in order to estimate

[27]RY Dougnon and others 'Accurate Online Social Network User Profiling' in S Hölldobler, R Peñaloza, and S Rudolph (eds) *KI 2015: Advances in Artificial Intelligence. KI 2015. Lecture Notes in Computer Science* (Springer, 2015)

[28]Ian Kerr and Jessica Earle, 'Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy' (2013–2014) 66 SLRO 65, 69.

[29]V Kumar and others, 'Understanding the Role of Artificial Intelligence in Personalized Engagement Marketing' (2019) 61 CMR 135–55.

[30]'It's the middle of the night. Do you know who your iPhone is talking to?' *Washington Post* (Washington DC 28 May 2019) <https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/> accessed 18 October 2020.

whether the couple is likely to separate. This would be valuable if the analysis is sold to a bank which needs to decide whether to grant an applicant a loan, as evidence of possible financial instability. If a technology company's contract for free services with a phone user permits both user voice recordings and their analysis, it would be possible to utilise private conversations for data analysis. This can be used, perhaps while deciding whether to grant a loan or job to somebody. It could also be used for targeted advertising. For example, a person discussing an aspiration to take a vacation may receive increased holiday adverts. These matters, though seemingly unethical, would not necessarily be illegal, depending on the power of the technology company. Google hired futurist Ray Kurzweil to work on predictive algorithms, using all the data that Google has at its disposal.[31]

An individualised digital thought clone can be used first to predict how a person will behave in a given set of parameters based on very precise behavioural patterns. Once the thought clone makes such a prediction, it can be used to determine the factors that would require it to make a different decision. This is already being done by consumer behaviour clones, which can, for example, determine what to display on a website to affect the decision of a category of online shoppers, based on probabilities.[32] An example of this is predicting whether a person will make an effort to conduct an online price comparison for a purchase, and if they do not, charging a premium for their chosen purchase. Such 'dark patterns'[33] manipulate a person's online choices[34] and reduce their decision-making independence through information overload or data invisibility.[35] While predictions can have high levels of accuracy, they are still based on profiling a person. A thought clone would not categorise a person into a profile to predict a decision but would rather use all available factors to determine the likely decision the user would make, allowing marketers to deploy techniques to further influence their decisions, such as consumer purchases. This is known as digital manipulation, which can reduce a person's ability to make choices freely.[36]

Humans and machines learn and make decisions differently (see Danks on the difference between human and machine learning),[37] but machines can learn to replicate human decision-making processes based on patterns. This can be used to automate

[31]City AM (n 8) 65. On regulating the use of AI in the financial sector, see Jon Truby, Rafael Brown and Andrew Dahdal, 'Banking on AI: mandating a proactive approach to AI regulation in the financial sector' (2020) Law and Financial Markets Review 14(2).

[32]Maurice E Stucke and Ariel Ezrachi, 'Artificial Intelligence & Collusion: When Computers Inhibit Competition' (2017) UILR 1775; Jack Caravelli and Nigel Jones, *Disruption: Big Data, Artificial Intelligence and Quantum Computing, Chapter in Cyber Security: Threats and Responses for Government and Business* (Praeger Security, 2019).

[33]' … user interfaces that have been intentionally designed to sway (or trick) users towards taking actions they would otherwise not take under effective, informed consent'. US Senate Intelligence Committee Vice Chairman, 'Potential Policy Proposals for Regulation of Social Media and Technology Firms' <https://www.warner.senate.gov/public/_cache/files/d/3/d32c2f17-cc76-4e11-8aa9-897eb3c90d16/65A7C5D983F899DAAE5AA21F57BAD944.social-media-regulation-proposals.pdf> accessed 11 February 2020.

[34]Robert Gorwa, 'Computational Propaganda in Poland: False Amplifier and the Digital Public Sphere' (2017) Oxford Internet Institute, University of Oxford, Working Paper No. 2017.4.

[35]B Kamleitner and VW Mitchell 'Can Consumers Experience Ownership for their Personal Data? From Issues of Scope and Invisibility to Agents Handling our Digital Blueprints' in J Peck and S Shu (eds), *Psychological Ownership and Consumer Behavior* (Springer, 2018).

[36]F Pasquale, *The Black Box Society: the Secret Algorithms that Control Money and Information* (Harvard University Press, 2015).

[37]D Danks, 'Learning' in K Frankish and W Ramsey (eds), *The Cambridge Handbook of Artificial Intelligence* (Cambridge University Press, 2014).

human skills by learning from the choices they make in various scenarios to remove the need for human involvement in each task.

Sammut explained that '[b]ehavioral cloning is a method by which human sub-cognitive skills can be captured and reproduced in a computer program. As the human subject performs the skill, his or her actions are recorded along with the situation that gave rise to the action. A log of these records was used as input to a learning programme. The learning program outputs a set of rules that reproduce skilled behaviour'.[38] Tasks that would be unmanageably slow with human involvement in every decision can be automated by learning from human decision-making patterns.[39] In recognising the ability of the software to clone a human's decision-making pattern, this creates a far broader opportunity to develop individualised clones that can predict a particular human's decision-making in other instances such as consumer behaviour. This already exists in the automotive industry, where AI can monitor a particular driver's driving styles to replicate it in the automated self-drive mode.

A recently submitted patent application by Ivanov indicated that the '[v]irtual cloning of human beings is being explored for various purposes in the industry'.[40] The patent application proposes 'a digital virtual clone of a user that learns about user and effectively functions on the behalf of the user'.[41] This explains the proposal Figure 2:[42]

> The first computing system designs a virtual clone of the user using the organised user information and produces a digital virtual clone of the user. A storage device stores organised user information. A second computing system generates and displays a simulated environment. The second computing system transfers the organised user information, integrates the organised user information, and displays the digital virtual clone of the user in the simulated environment, wherein the digital virtual clone interacts with the stimulated environment.[43]

The above patent application essentially describes a digital thought clone. Such thought cloning moves on from profiling to cloning a person's unique decision-making patterns and combining them with existing available data, thus creating a clone with the closest possible similarity to the person in question. AI algorithms can then simulate how the clone would respond to a given set of circumstances, such as what purchasing decision it would make when given certain choices. With technology users willing to trade their personal data for free and convenient use of apps, search engines, and cloud services, data miners have managed to exploit these data for use in predictive technologies. Zuboff referred to this as the commercialisation of 'decision rights'[44], as the 'agency we can actively assert over our own futures, which is fundamentally usurped by predictive, data-driven systems'.[45]

---

[38]C Sammut, 'Behavioral Cloning' in C Sammut and GI Webb (eds), *Encyclopedia of Machine Learning and Data Mining* (Springer, 2017).

[39]' … capturing, cloning and patenting essential parameters of the decision models from a particular human expert making these models transparent, proactive and capable of autonomic and fast decision-making simultaneously in many places'. Vagan Terziyan, Svitlana Gryshko, Mariia Golovianko, 'Patented intelligence: Cloning human decision models for Industry 4.0' (2018) 48 JMS 204.

[40]Yevgen Ivanov, 'System and method for using a digital virtual clone as an input in a simulated environment', *US9959497B1* (1 May 2018) <https://patents.google.com/patent/US9959497B1/en> accessed 18 October 2020.

[41]ibid.

[42]Ivanov (n 38).

[43]ibid.

[44]S Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2018).

[45]Zuboff (n 1).

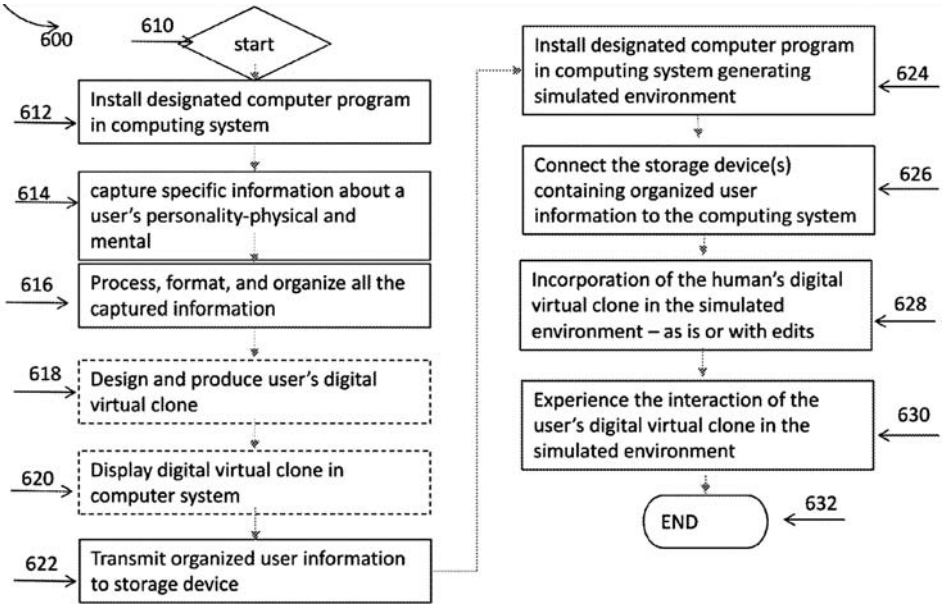

Figure 2. Example of a patent application for a digital thought clone.

Collated and behavioural tracking data fed into an AI digital thought clone would offer a highly individualised and consequently lucrative service to businesses and governments aside from limited marketing purposes. Financial institutions can use these data to make financial decisions, such as determining whether a person would repay a loan, rather than deciding on a person's statistical profile. Insurance companies can use them to determine whether a person is eligible for medical insurance by predicting the likelihood of future illnesses by taking into account factors such as spending data (providing information on diet and gym membership), the distance a person walks in a day (based on their phone's location history), their online searches demonstrating their level of health education, and other influential factors such as their social group, based on their phone contacts and social media groups. Tax authorities can work out individual profiles with around-the-clock monitoring of payments, rather than conducting randomised tax inspections on individuals and corporations. Similarly, crime prevention agencies can use real-time data such as online searches, spending patterns, online posts, and match this with AI-image recognition to predict those who need additional screening. The collected data could predict the likelihood of mental health issues arising from factors such as family history, medical records, the user's physical and digital social interactions (with flags for warning signs of unusual behaviour), and online behaviour such as the types of news consumed and shopping habits. The real-time location of a user can be matched with other physical factors to identify whether they have a vitamin D deficiency, which may increase the likelihood of depression. It can also help identify whether a person gets enough physical activity or frequents bars and is thus susceptible to alcoholism. This can help health providers intervene when a person is flagged. For example, in a viral pandemic such as COVID-19, virologists can track the movements and interactions of people who may have been exposed to the virus, thus requiring quarantine. It also

means that a person's data can be used against their interests by health insurance providers who may wish to charge a higher premium or exclude higher-risk candidates from coverage.

Engineers develop virtual replicas of physical entities known as 'digital twins', in order for AI to run simulations before testing in the real world.[46] This could be the 3D-modelling, for example, of a planned bridge, or a digital twin of a city to predict its ability to cope with the rise in water level over time. Britain's National Infrastructure Commission created digital twins of all of the United Kingdom's national infrastructure to identify ways to deal with challenges such as climate change and increased population.[47] Cities like Singapore and Newcastle-upon-Tyne have created digital twins to help with planning, such as for energy needs and disaster management, which has enabled testing and planning in multiple scenarios.[48]

Rather than digital twin cities, this article identifies the potential or actuality of a digital twin being built to replicate human data and behaviour, in order to predict or influence a person's decisions. For instance, election pollsters can not only predict voting intentions, but can also try to alter them, by testing how interventions such as certain news stories displayed on a user's computer may affect their decision, in a simulated environment. This can then be applied outside of the clone to the real person.

With data concerning a subject that is continually trawled, the digital clone would be a continually updated real-time version of the person, monitoring both the person's changing views and behaviour, as well as the type of interactions that successfully affect their behaviour. For instance, AI-driven persuasive algorithmic software can continually try different ways to identify the type of digital advertisements that can persuade a person to change their online purchasing behaviour. This provides a more accurate and real-time understanding of approaches that can work in the future and that can allow AI to predict a user's behaviour more accurately and target interventions such as advertisements, news stories, or search engine results more effectively in the future.

At the time of this writing, the technology to enable such digital thought cloning either existed under an unpublicised name or will inevitably exist in the near future. The term 'digital thought cloning' is therefore novel to this article.

3. Theories of data privacy

A discussion of the legal and ethical implications of digital thought clones must necessarily be preceded by a discussion of the theories underlying data privacy in order to analyse digital thought clones within a given framework. This is because legal and ethical approaches to digital thought clones, which largely raise issues related to ownership, control, and rights to personal data, will be driven by underlying theoretical assumptions of privacy. These assumptions are often expressed under the two prevailing theories of privacy, namely the public/private dichotomy and the contextual integrity theory. This

[46]'What is a digital twin and why it's important to IoT' *Network World* (City 31 January 2019) <https://www.networkworld.com/article/3280225/what-is-digital-twin-technology-and-why-it-matters.html> accessed 26 October 2020.

[47]'Cambridge University Centre for Digital Built Britain, National Digital Twin Programme' (Cambridge) <https://www.cdbb.cam.ac.uk/national-digital-twin-programme> accessed 26 October 2020.

[48]'How the UK is creating a digital twin to deal with climate change and population growth' *NS Business* (London 23 January 2019) <https://www.ns-businesshub.com/editors-pick/what-is-a-digital-twin-uk/> accessed 26 October 2020

article argues that these two prevailing theoretical views of privacy fall short when applied to AI and digital thought clones that require the pervasive and continuous use of a person's data in both public and private spheres of overlapping contexts. This article argues that effective legal protection of personal data can only work under a human-centred approach to data privacy.

3.1. Prevailing theories of data privacy

There are currently two dominant views on data privacy: the public/private dichotomy and the contextual integrity theory.

3.1.1. Public/private dichotomy

The dominant theory regarding privacy, at least in the US, and one most recognised by leading privacy scholars is the view of privacy as a question of whether information is public or private.[49] This view has long shaped policies and regulations concerning the privacy of persons, property, information, and eventually, electronic data.

In the US, the public/private dichotomy shaped privacy analysis in three ways: (1) preventing unwanted governmental intrusion, (2) protecting information deemed sensitive, and (3) protecting spheres deemed private or personal.[50] While the US Constitution does not make any specific reference to privacy, the US Supreme Court has recognised penumbras from a number of constitutional provisions that form a zone of implicit privacy rights.[51] The US Supreme Court has recognised privacy as a fundamental right, holding governmental regulations at a higher standard of scrutiny with respect to marriage,[52] procreation,[53] child rearing and education,[54] use of contraception,[55] abortion,[56] homosexual activity,[57] obscenity in the home,[58] certain family relationships,[59] and refusal of medical treatment.[60] In these cases, the US Supreme Court found that the right to privacy operates, as the decisions affected personal and private spheres that fit within the public/private dichotomy. The application of the US Fourth Amendment's search and seizure applies a public/private dichotomy, as the US Supreme Court set out the rule in *Katz v. United States*[61] that the Fourth Amendment only protects people against governmental intrusion when there is a 'reasonable expectation of privacy'. As Justice Stewart stated in *Katz*,[62] 'What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection'.

[49]Nissenbaum (n 4)
[50]ibid.
[51]Griswold v. Connecticut, 381 US 479 (1965).
[52]*Loving v. Virginia*, 388 US 1 (1967).
[53]Skinner v. Oklahoma ex rel. Williamson, 316 US 535 (1942).
[54]Pierce, Governor of Oregon, et al. v. Society of the Sisters of the Holy Names of Jesus and Mary, 268 US 510 (1925); Meyer v. Nebraska, 262 US 390 (1923).
[55]*Griswold v. Connecticut*, 381 US 479 (1965) (recognizing the right of married couples to purchase contraceptives); *Eisenstadt v. Baird*, 405 US 438 (1972) (the right of individuals to purchase contraceptives).
[56]*Roe v. Wade*, 410 US 113 (1973); *Planned Parenthood v. Casey*, 505 US 833 (1992).
[57]*Lawrence v. Texas*, 539 US 558 (2003).
[58]*Stanley v. Georgia*, 394 US 557 (1969).
[59]Prince v. Massachusetts, 321 US 158 (1944).
[60]Cruzan v. Director, DMH, 497 US 261 (1990).
[61]389 US 347 (1967).
[62]*Katz v. United States*, 389 US 347 (1967).

With the advent of new technology, the public/private dichotomy has allowed the government to have access to information on individuals through the use of surveillance technology, by courts interpreting emails and online activity as public, and by redefining sensitive information as public.[63]

3.1.2. Contextual integrity theory

Nissenbaum, after pointing out the shortcomings of the public/private approach to privacy protection, proposed a normative conceptualisation of privacy that focuses on the context of the information, called contextual integrity. According to Nissenbaum, there ought to be privacy protection of information if 'one or the other types of the informational norms has been transgressed'.[64] The contextual integrity approach to privacy examines norms to decide key contextual aspects of the information like the 'roles, expectations, behaviors, and limits' that a person usually attributes to such information.[65]

Contextual integrity also examines the appropriateness of information in a given context, and the distribution or movement of information. Appropriateness looks into the type of information that is deemed private by determining the norm for what is allowed, expected, or required in a given context. Only certain kinds of information sharing, for example, would be appropriate while buying groceries versus visiting a doctor. The distribution of information determines who may have access to it by examining the relationships of the parties to the information flow.

Nissenbaum provided an example of how contextual integrity would apply in a similar context, albeit in a very limited sense, to that of digital thought clones. She used consumer profiling and data mining as an example of when contextual integrity may apply.[66] In the example, she explained that appropriateness would be breached when a merchant asks questions about lifestyle choices such as vacations, movies watched, books read, and schools attended. However, according to Nissenbaum, a merchant like Amazon asking questions to determine what customers want and thereby improving their marketing would be appropriate. She also stated that merchants would be responsible for the flow of information, meaning that they would breach distribution norms if they shared the information with third parties.

3.1.3. Inapplicability of prevailing theories to digital thought clones

The prevailing theoretical frameworks of privacy may lead to the absence of privacy protection when applied to the use of AI in digital thought clones.

The public/private dichotomy may lead to a virtual lack of privacy protection of data in digital thought clones because such data would be deemed public. For the same shortcomings identified by Nissenbaum, the public/private dichotomy approach has led to a view of privacy that renders new technology public because electronic data have been interpreted under this framework as existing in the public sphere, despite the fact that the data involve personal information and were created in a private setting. The public/private dichotomy has viewed emails and online activity as public activities because the data are processed, controlled, and stored in public places such as the

[63]Nissenbaum (n 4) 131–4.
[64]ibid., 138
[65]ibid.
[66]ibid., 152–4.

servers of Internet service providers. Such an analysis allowed the US government to conduct mass surveillance of Internet traffic. Further, individuals who created the data may not be deemed the owners of such data, which are stored on servers owned by third parties. As digital thought clones comprise a collection of data (emails, online traffic, social media activities, and data on apps and software owned by third parties) stored by major technology firms ('Big Tech')[67], the public/private dichotomy interprets digital thought clone data as comprising public data with no reasonable expectations of privacy.

The contextual integrity theory provides a more promising framework for protecting privacy in digital thought clone data because it requires revisiting the appropriateness of the use of data. However, contextual integrity can lead to minimal privacy protection when applied to digital thought clones because the use of data in this context involves pervasive and continuous use of a person's data in overlapping contexts.

The use of data in digital thought clones is pervasive because digital thought clones use data about a person from every aspect of their life to the extent that digital thought clones can replicate their personality, behaviour, and choices, and become a digital twin. Determining the appropriateness of each type of data in such a pervasive use would render the contextual integrity analysis ineffective because data are used in a limitless number of contexts.

The use of data in digital thought clones is often continuous and overlaps with other data sets. In this sense, the use of data in digital thought clones may constantly change in context, blurring the appropriateness and distribution of information. Data stored in a database, for example, may be accessed concurrently for multiple varying purposes and roles because of the way in which AI-driven software processes such data. In deep neural network types of AI algorithms, for example, how the algorithm processes the data remains unknown. In machine learning, the algorithm stores data for learning purposes, and builds on them by predicting future behaviour.

Nissenbaum's example of the use of consumer data by Amazon for marketing as appropriate under contextual integrity is exactly the type of framework that would allow the creation of a digital thought clone for the given pre-textual purposes of marketing. It would, however, be marketing that is so accurate because it creates a digital twin for each consumer.

3.2. Human-centred approach to data privacy

A framework for privacy protection in the context of digital thought clones would have to look to the person as the source of privacy protection rather than examining both the use of information in a public or private sphere and the context backing the use of such information. Regardless of where the information is being used and of its appropriateness and distribution, individuals should be able to determine, while creating the data, whether such data are to be treated as requiring privacy protection in perpetuity or until they waive it. This is called the human-centred approach to data privacy, where the decision on whether data should be protected by privacy regulations either rests in the hands of the individual creating the data or depends on what the data are about.

[67] Andreas Stegmann, 'What is (Big) Tech? A Taxonomy' *Medium* (City 4 March 2020) <https://medium.com/hyperlinked/what-is-big-tech-a-taxonomy-af17c3aff88d> accessed 23 September 2020.

The presumption in a human-centred framework of data privacy is that data belong to the person, and that certain data about a person are inherently protected. This is the principle of ownership. There is also a control principle, which places a requirement that individuals must be allowed to make changes to the type of data and whether data can be stored. The human-centred approach applies an access notice principle, where individuals should be notified before data are shared with an entity that has not been authorised for access previously. Finally, the human-centred approach requires an individual to actually give consent to the use of data regardless of the context, and of the public or private sphere of use.

The human-centred approach is consistent with the EU's recognition of the fundamental right to data protection, as embodied in national legislation and European Union law like the EU GDPR.[68] This is consistent with the view that the right to privacy is a human right, and that discriminatory practices can stem from unregulated data. The GDPR[69] and the California Consumer Privacy Act of 2018[70] (CCPA), discussed further below, already cover many principles of the human-centred approach. For this reason, these two legislations can be seen as moments in data protection legislation when there has already been a shift in how people view the privacy of their data from the previous frameworks towards a more human-centred approach.

4. Potential legal issues in digital thought cloning

The practice of creating AV digital, consumer behaviour, and digital thought clones as well as mindclones poses legal and ethical issues that this article proposes ought to be brought to the fore for public discussion and scrutiny.[71] This section discusses the myriad of potential legal issues raised by digital clones, particularly digital thought clones. This article does not aim to resolve these legal issues but has a more modest aim of encouraging further discussion around both these and other issues that we have not identified thus far. Digital and digital thought clones raise legal issues relating to data privacy, informed consent, anti-discrimination, copyright, and right of publicity. This section discusses the application of existing legal standards to digital thought clones in jurisdictions like the EU and the US.

4.1. Data privacy

Within the EU, the right to data protection and respect for private life are provided under Articles 7 and 8 of the EU Charter of Fundamental Rights, respectively. Under Article 4(1) of the GDPR, 'an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person'. There are various legal requirements in the GDPR as well as in other jurisdictions

[68]Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.
[69]ibid.
[70]TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199].
[71]N Bostrom and E Yudkowsky, 'The ethics of artificial intelligence' in K Frankish and W Ramsey (eds), *The Cambridge Handbook of Artificial Intelligence* (Cambridge University Press, 2014).

such as the CCPA, to protect the subject's data and privacy during its storage and processing, and to avoid algorithmic discrimination.[72]

Both the GDPR and CCPA provide definitions of pseudonymisation[73] or anonymisation.[74] Essentially, the difference is that 'Pseudonymous data still allows for some form of re-identification (even indirect and remote), while anonymous data cannot be re-identified'.[75] Where a subject's data are pseudonymised or anonymised, it may be possible to utilise the data for analytics or research without falling foul of the regulations. The US Senate Intelligence Committee recognises this as a means of protecting personal data.[76] Neither the GDPR nor the CCSP apply to anonymised data ('deidentified' data in the CCSP), given that the data can no longer identify the data subject.[77]

However, where the intention of the technology is to create a personalised profile of a person, this would be included within the scope of the regulations. Such digital thought cloning referred to in this article is foreseen as a risk to natural persons caused by data processing in Recital 75 of the GDPR, 'where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles'[78] Types of personal data referred to include 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures'.[79] Thus, the GDPR imagines the inclusion of multiple different types of personal data being used in a digital thought clone, and a person's data being used against their interests based on existing human biases to automate decisions. The forward-thinking nature of the GDPR means that any technology attempting to create a digital thought clone involving an EU citizen's personal data would be classed as a risk to natural persons because it could cause damage to the person, and such risks are subject to an objective risk assessment, including a plan to mitigate the risks.[80] The GDPR defines 'damage' broadly, and includes damage such as discrimination and financial loss. Financial loss may occur where the personalised profile is utilised by the AI software to charge a premium to

[72]C O'Neilly, *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy* (Allen Lane, 2016).

[73]' … 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'. Article 4, GDPR. CCSP covers this in Sections 1798.100(e), 1798.140(r), 1798.145(i).

[74]' … information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'. Recital 26, GDPR

[75]'The legal distinction between anonymised and pseudonymised data is its categorisation as personal data. Pseudonymous data still allows for some form of re-identification (even indirect and remote), while anonymous data cannot be re-identified'. PrivSec Report, 'Data masking: Anonymisation or pseudonymisation?' *PrivSec Report* (November 7, 2017) <https://gdpr.report/news/2017/11/07/data-masking-anonymisation-pseudonymisation/#:~:text=The%20legal%20distinction%20between%20anonymised,data%20cannot%20be%20re%2Didentified> accessed 23 September 2020.

[76]'Business processes that handle personal data would be built with data protection by design and by default, meaning personal data must be stored using pseudonymisation or full anonymization'. See FN32.

[77]For further comparison of GDPR and CCSP, see 'DataGuidance and Future of Privacy Forum, Comparing privacy laws: GDPR v. CCPA' *FPF* (Washington, DC, 18 December 2019) <https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf> accessed 24 September 2020.

[78]Recital 75, GDPR.

[79]Recital 75, GDPR; GDPR, art 9(1).

[80]For an explanation and analysis see A Spina, 'A Regulatory Marriage de Figaro: Risk Regulation, Data Protection, and Data Ethics' (2017) 8 EJRR 88–94.

the person for a product bought online, or to deny them a job or a loan. Being discriminated against is also classified as damage. The GDPR regulates the use of personal data to influence behaviour while using autonomous and analytics software, when the data used include EU subjects. The CCPA also deems 'charging different prices or rates for goods or services' based on the person's data to be an illegal form of discrimination.[81] This should consequently prohibit types of algorithms that utilise user data to manipulate prices offered to charge a premium, known as personalised algorithmic pricing.[82] The UK's Competition and Markets Authority also identified that risk that '… personalised pricing, directed marketing and behavioural discrimination have become a possibility for companies with large datasets'.[83]

An additional type of damage included in Recital 75 of the GDPR is 'where data subjects might be … prevented from exercising control over their personal data'. Article 25 of the GDPR seeks to protect against this risk by placing obligations on an organisation's data controller to '… implement data protection principles, such as data minimization' (GDPR Article 25(1)) and by requiring that '… by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons' (GDPR Article 25(2)). If a digital thought clone is actually considered the personal data of an EU citizen, then that citizen would have the right to access, and perhaps opt out from its use. The requirement to allow people to opt out, as they can now do with other uses of their data pursuant to the GDPR, would alert them to the existence of a digital thought clone. If this is understood, it would be both alarming and frightening for the person. The GDPR gives data subjects the ability to withdraw consent to use their data and the ability to object to its use for marketing or other legitimate purposes,[84] whereas the CCSP provides data subjects with the right to opt out of selling their personal information.[85]

Another damaging use of the potentially discriminating data under Recital 75 of the GDPR would be 'where data subjects might be deprived of their rights and freedoms … '. The EU Charter of Fundamental Rights guarantees rights to EU citizens, including data protection (Article 7), freedom of expression (Article 11), and respect for private life (Article 7). If behavioural tracking software is indeed impacting a person's private life, for example – which would be perfectly possible through multiple means of monitoring and recording a person's private behaviour – it could be classed as a type of potential damage in violation of the Recital. If a person's online expressions were used to form their profile, which denied them some benefits, it could be considered damage. Other types of freedoms would also be relevant, including the freedom of movement within the EU, established in the Treaty of Maastricht 1992. Kerr and Earle discussed the possibility of predictive algorithms generating no-fly lists.[86] If a predictive AI-driven algorithm developed a personalised profile of a person that flagged them as a travel security risk and

[81]Section 1798.125.
[82]P Seele and others. 'Mapping the Ethicality of Algorithmic Pricing: A Review of Dynamic and Personalized Pricing' 2019 JBE <https://link.springer.com/article/10.1007/s10551-019-04371-w#citeas>
[83]'Pricing algorithms Economic working paper on the use of algorithms to facilitate collusion and personalised pricing' *UK Government* (London 8 October 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_report.pdf> accessed 24 September 2020.
[84]GDPR Articles 12, 21 Recital 70.
[85]Sections 1798.120, 1798.135.
[86]City AM (n 8) 69.

that analysis was used to stop the person from travelling, it may be deemed to cause damage to the person under the GDPR and consequently be an illegal use. As Kerr and Earle identified, predictive algorithms used in countering crime could undermine the presumption of innocence.[87]

European courts have already used the EU Charter of Fundamental Rights to limit European governments' abilities to collect and process personal data concerning citizens, even in the name of counter-terrorism. The UK enacted the Data Retention (EC Directive) Regulations 2009,[88] which incorporated the European Commission's Data Retention Directive (2006/24/EC)[89] into British law. This required communication service providers to retain communications data for a year, including all emails, mobile phone, online, and landline phone communications. Communication service providers were further required to store the time and date of the communication, the details of the recipient, the sender's geographical location including their direction of travel, and any data that could identify the sender. In *Digital Rights Ireland and Seitlinger et al.*, Joined Cases C-293/12 and 594/12, 8 April 2014, the European Court of Justice (ECJ) ruled that the Directive was not valid, largely because the requirement to collect such data for everybody indiscriminately was a disproportionate measure to counter terrorism.[90] Trawling everybody's personal data, even in the name of security, would have amounted to a breach of privacy rights as even people who were not under investigation would have had all their telecommunications monitored and processed.

The GDPR does not completely prevent all risky technologies and uses of data but does require risk assessment alongside risk mitigation measures. This would ultimately rule out some uses of technology. Nevertheless, because of the GDPR, CCSP, and ECJ rulings, there are multiple potential uses of technology that would not be permitted for EU citizens. The ability of a software developer to create a digital thought clone of an EU citizen that would be permitted in the EU is considerably limited by the GDPR.

4.2. Informed consent

The GDPR has gone far to protect EU citizens from their data being processed without their consent, with a number of distinct and clear requirements for data controllers. For an EU citizen's personal data to be processed legally, GDPR Recital 40 requires consent, and sets out an exhaustive list of other lawful bases for processing. Consent may be the simplest requirement to fulfil, though it must be a freely given, specific, informed, and an unambiguous indication of the data subject's wishes'.[91] The use of the data must be clearly set out for the consenting party. Google was penalised by France's National Data Protection Commission with a €50 million fine for failing to achieve this.[92] 'Freely given' means that it cannot be in exchange for using a service.[93]

[87]ibid.
[88]The Data Retention (EC Directive) Regulations 2009 (SI 2009/859).
[89]Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63.
[90]Pursuant to Articles 7, 8, and 52(1) of the EU Charter of Fundamental Rights.
[91]GDPR Article 4(11).
[92]'Why France hit Google with a whopping €50 million fine' *The Local* (Paris 21 January 2019) https://www.thelocal.fr/20190121/why-france-fined-google-50-million
[93]GDPR Recital 42, as defined in Recital 43.

Consent is required by the GDPR for each specific type of use, such as obtaining an email address for marketing. The request for consent must be readily understandable: it cannot be vague, confusing, or unclear,[94] and cannot be construed from '[s]ilence, pre-ticked boxes or inactivity … '[95] To fulfil the requirement of 'specific and informed' consent, the identity of the data controller must be clear (Recital 42), as must the purposes (Recital 43) and processing activities. The person should also be capable of withdrawing consent at any time, although there is no time limit on a person's consent provided that it remains reasonable to retain such data. The CCSP requires businesses to inform customers before or at the point of collection, of the categories of the personal data to be collected and the purposes for which such data are used.[96]

Developing a digital thought clone within the EU or California would consequently face considerable legal challenges. Nevertheless, the number of users simply accepting requests for consent without consideration, in order to quickly access the services they desire, means that, in reality, legal protection would not prevent this form of AI. Despite legal protection in the GDPR, people often do not take the time to read privacy policies[97] given their length and the number of privacy policies each person would have to read. It is estimated that it would take 244 h a year for data subjects to read all the privacy policies they are faced with.[98] Custers noted that '[a]s a result, Internet users seem to become increasingly disengaged in the consent processes'.[99]

4.3. Anti-discrimination laws: encouraging behavioural cloning

Existing algorithms that automate the outcome of a decision through statistical profiling[100] have faced legal difficulties, where there is a possibility of a discriminatory outcome for a person.[101] In a case before a Finnish tribunal, a bank used profiling software that resulted in an automated decision that rejected a person's credit application. The automated decision-making algorithm used data factors such as gender, language, and age to determine whether the credit applicant was ineligible. As this was discriminatory, the National Non-Discrimination and Equality Tribunal ruled that it had violated Finland's Non-Discrimination Act (1325/2014).[102] Instead, an individual assessment of the applicant was found to be the only fair means of determining eligibility, placing an increased onus

[94]UK Information Commissioner's Office: 'If the request for consent is vague, sweeping or difficult to understand, then it will be invalid'. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/.

[95]GDPR Recital 32.

[96]CCSP Sections 1798.100(b), 1798.130(a), 1798.135.

[97]DJ Solove, 'Privacy self-management and the consent dilemma' (2013) 126 HLR 1880.

[98]AM McDonald and LF Cranor, 'The cost of reading privacy policies,' (2008) 4 I/SJLPIS.

[99]B Custers, 'Click here to consent forever: Expiry dates for informed consent' (2016) 3 BDS.

[100]Article 4(4) GDPR defines 'profiling as ' … any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

[101]C O'Neilly, *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy* (Allen Lane, 2016). On the subject of preventing discriminatory outcomes in AI decision-making see Jon Truby, 'Governing Artificial Intelligence to benefit the UN Sustainable Development Goals' (2020) Sustainable Development 946.

[102]National Non-Discrimination and Equality Tribunal of Finland/Plenary Session (voting), 'Assessment of creditworthiness, authority, direct multiple discrimination, gender, language, age, place of residence, financial reasons, conditional fine' 216/2017. https://www.yvtltk.fi/material/attachments/ytaltk/tapausselosteet/45LI2c6dD/YVTltk-tapausseloste-_21.3.2018-luotto-moniperusteinen_syrjinta-S-en_2.pdf.

on the bank as this would be more time-consuming and costly to carry out. Similarly, where a decision would result in a legal effect on a data subject, the GDPR[103] does not allow automated decision-making based on statistical profiling because this would be unfair to the person.[104] The GDPR identifies a risk of 'significant economic or social disadvantage' caused by data processing, which poses a threat to the rights and freedoms of natural persons.[105]

This creates a legal motivation for organisations to develop individualised profiles that can provide a rationale for a decision affecting a data subject that is personalised and not based on profiling. As Article 22(1) would require a human to be involved in the decision-making process affecting a person rather than being completely automated, there is also a motive for organisations to use AI to provide a human decision-maker with as much information as possible on the person, to save the cost and time of employing a human to collate and analyse all the information.[106] Rather than an employee of a bank, for example, collating all required data for an individual (non-profiled) assessment of a loan application, AI can provide all the required information instantly by accessing a pre-developed digital clone of the data subject. The human can still make the final decision and meet the legal requirement to 'inform' (rather than provide an explanation[107]) the data subject of the factors applied and rationale for making that decision. Consequently, there is a strong business case that utilises digital clones to comply with the GDPR. It would also be possible for simulations to be run on the digital twin version of the person, to test eventualities such as financial difficulties in the case of marital breakdown, allowing financial institutions to factor in risks in their decision-making.

4.4. Copyright law

Another question is whether digital and digital thought clones can be protected under copyright law. Copyright law, at least in the US, requires originality and creativity. US Copyright Law protects copyright in 'original works of authorship fixed in any tangible medium of expression'.[108] In *Feist Publications, Inc. v. Rural. Serv. Co.*,[109] the US Supreme Court held that a work must be original to qualify for copyright protection. The *Feist* judgement also required that the author must independently create, rather than copy from other works, some threshold amount of material, and the work must possess some minimal degree of creativity.[110] The only case in the US that has addressed the issue of copyright protection for digital models is *Meshwerks*

[103]Article 22(1) of the EU's General Data Protection Regulation: 'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'.
[104]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/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, pp. 1–88).
[105]Recital 75, GDPR.
[106]Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 IDPL 76; Emily Pehrsson, 'The Meaning of the GDPR Article 22' (2018) 31 EULWP (2018).
[107]Wachter and others, ibid.
[108]17 USC. § 102 (2008).
[109]Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 US 340 at 350 (1991).
[110]Feist, 499 US at 345.

v. Toyota,[111] where the Tenth Circuit Court of Appeals held that digital copies, like photographs, are not protected under copyright law if they do not meet the minimal degree of originality despite the efforts used in creating the models.[112] Digital thought clones are not mere digital copies, unlike the digital copies of design in the *Meshwerks* case, as AI algorithms arguably possess some minimal degree of creativity and engage in independent creation of predictions and analysis of the digital data. While the digital thought clone system itself may be protected by copyright, the data fed into the AI system may not be so if they are mere digital copies, and especially if they are in the public domain.

In the UK and Australia, on the other hand, digital copies involving the exertion of a substantial amount of time, skill, and effort may be protected under their respective copyright laws.[113] Both the UK and Australia, unlike the US Supreme Court in *Feist*, recognise the principles of industrious collection and 'sweat of the brow'.[114] In the UK, for example, the court in *Sawkins v. Hyperion Records, Ltd.*[115] applied the 'sweat of the brow' principle and held that reproductions requiring talent and skill are copyrightable. For the *Sawkins* court, the question was the degree of labour, skill, and judgement in making the copy, considering both the sweat of the brow and individual creative input.

In Australia, the federal court in *Telstra Corp. Ltd., v. Desktop Marketing Systems Pty. Ltd.*,[116] a case involving a similar set of facts as in *Feist*, held that telephone directories are original and granted them copyright protection. The *Telstra* court expressly rejected the *Feist* approach and followed the English 'labour and expense' approach.[117] It granted copyright protection because of the substantial labour and expense involved in creating the directory.

Applying the principles of industrious collection and 'sweat of the brow,' courts in the UK and Australia may grant copyright protection to digital clones if their creation involved a substantial amount of labour, effort, skills, and expense. The UK and Australia are likely to grant copyright protection to the entire digital thought clone system, including the AI algorithm and the underlying data collection on each individual. They may allow companies to have greater ownership and control over a digital thought clone.

Whereas the EU is also not likely to grant copyright protection, it may do so under some dual copyright and *sui generis* regimes.[118] European Union Directive 96/9/EC,[119] which addresses the legal protection of databases, grants *sui generis* protection for copyrightable and uncopyrightable data that have economic value if the creator made a qualitatively or quantitatively substantial investment in setting up the database.[120] Companies that develop digital clones may be able to establish a substantial investment in creating them, especially digital thought clones.

[111]Meshwerks v. Toyota, 528 F.3d 1258 (10th Cir. 2008).
[112]Bryce Clayton Newell, 'Independent Creation and Originality in the Age of Imitated Reality: A Comparative Analysis of Copyright and Database Protection for Digital Models of Real People' (2010) 6 BYUILM 93.
[113]ibid.
[114]ibid.
[115]Sawkins v. Hyperion Records Ltd., [2005] EWCA 565, ¶ 1.
[116]Telstra Corp. Ltd., v Desktop Mktg. Sys. Pty. Ltd., [2001] FCA 612.
[117]ibid., 85.
[118]Clayton Newell (n 108).
[119]Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, 1996 O.J. (L 77) 20 <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML> accessed 8 January 2020.
[120]Clayton Newell (n 108); Joseph Beard, 'Clones, Bones and Twilight Zones: Protecting the Digital Persona of the Quick, the Dead and the Imaginary' (2001) 16 BTLJ 1165.

4.5. Right of publicity

When a digital clone or deepfake is made of a person without their consent, the enforcement of the right of publicity may be sought in certain US states such as California or New York.[121] The right of publicity protects against the unauthorised use of a person's likeness for commercial or advertising purposes, and gives the right to individuals to control the use of their voice, image, and other aspects of their personality for commercial purposes.[122] The right can be claimed post-mortem, such as in the unauthorised commercial use of a dead actor's image or likeness.[123]

The commercial or advertising use of a deepfake or digital clone thus falls under the scope of the right of publicity depending on the jurisdiction, where some may require a profit aspect to the owner's personality and the right may not be applicable to ordinary people. In the US, the state granted that the right of publicity can be limited under the First Amendment and can even be pre-empted by federal copyright law.[124] In some jurisdictions like the UK, the right of publicity is not even recognised.

When applied to a digital thought clone, the right of publicity may be used by celebrities and public figures who may be able to establish a profit aspect to the clone. For ordinary people who are unlikely to argue a profit aspect, the right of publicity will be difficult to establish.

Even for celebrities and public figures, if the digital thought clone itself is not being used for publicity but for mere prediction and analysis of the individual's behaviour, decisions, personality, and thoughts, then the right of publicity will be of limited use. It is entirely possible that a court may apply a broader right of publicity that can limit the use of a person's digital twin for commercial purposes without their consent or authorisation. This approach, however, is premised on the view that a digital clone, especially a digital thought one, is so similar to the human that it is inherently owned and part of the human's identity and legal personality. Courts may altogether create a new type of tort, such as the negligent or unauthorised use of a person's data.

5. Comparing biological and digital cloning

Just as biological cloning raises ethical dilemmas that led to the global moratorium on biological human cloning,[125] digital cloning raises equally important ethical issues. This article cannot possibly attempt to resolve these ethical issues. Instead, it sets a more modest goal of beginning to identify the potential ethical issues in order to spark discussions and encourage further research on them, and to enable the identification of additional ethical issues raised by the use of AI algorithmic data, process replication,

[121]Beard, ibid.; Kevin Goering and others, 'New York Right of Publicity: Reimagining Privacy and the First Amendment in the Digital Age - AELJ Spring Symposium' (2018) 36 CAELJ 601.
[122]ibid.
[123]Beard (n 116); Thomas McCarthy, *The Rights of Publicity and Privacy* (Boardman, 2000).
[124]Beard, ibid.
[125]Alfonso Gómez-Lobo, 'Human cloning: The ethical challenge' (2002) 5 EJB #; see also National Bioethics Advisory Commission, 1996–1997 Annual Report (1998) <https://bioethicsarchive.georgetown.edu/nbac/pubs/ann_rept.pdf> accessed 15 October 2020; Elisa Eiseman, National Bioethics Advisory Committee: Contributing to Public Policy (RAND 2003) <https://www.rand.org/content/dam/rand/pubs/monograph_reports/2007/MR1546.pdf> accessed 15 October 2020; US National Academy of Sciences, U.S. Policy-makers Should Ban Human Reproductive Cloning (18 January 2002) <https://www.nationalacademies.org/news/2002/01/us-policy-makers-should-ban-human-reproductive-cloning> accessed 15 October 2020.

and emergent technologies to create clones in the digital world. This section begins by first examining the ethical issues raised by biological cloning, so that there may be a point of reference within the larger discussion on the ethics of cloning. It then compares the ethical issues raised by biological cloning with those raised by digital cloning.

5.1. Ethical and moral issues in biological human cloning

To arrive at a better understanding of the ethical issues raised by digital cloning, it is necessary to understand, discuss, and compare the ethical issues raised by biological human cloning. A cursory discussion of the main arguments in ethics and morality pertaining to cloning is therefore necessary. In Western philosophy, arguments on the ethics and morality of cloning are based on two pillars. The first is the utilitarian principle that an act is morally right if it is conducive to the greatest good of the greatest number of people,[126] and the second is the ethical liberal norm that individuals must not engage in actions that entail harm to human beings, or 'do no harm' to others.[127]

The ethics and morality of biological human cloning have largely been examined by weighing the aims or goals of cloning against the utilitarian principle and the ethical liberal norm of 'do no harm'. While the underlying myriad of motivations and aims to create a biological human clone can constitute a complex phenomenon, these reasons have been categorised into two main conceivable goals: (1) complete human reproduction, and (2) human cloning for scientific and medical purposes.[128] The second has also been referred to commonly as therapeutic cloning or cloning for biomedical research.

The first goal of cloning for reproduction or generating a child has been universally deemed morally wrong from the ethical liberal norm of 'do no harm' because of the inherent dangers in the cloning procedure.[129] A very high percentage of cloned mammals have either died before or after birth, with a high percentage of abnormalities.[130] As no successfully cloned animal has ever been deemed perfectly normal, submitting a child to the harms of cloning would be morally wrong. Whereas some argue that reproductive cloning can be morally right someday if the procedure is safe, others argue that such a procedure could never be reached without subjecting such a cloned human being to the unconsented experiment, thus never making it morally right.[131]

The second goal of biological human cloning for therapeutic purposes has been argued under the utilitarian principle. Those in favour of therapeutic cloning like the Academy of Sciences argue that it is morally right because it is conducive to the greatest good of the greatest number of people.[132] Those who oppose it argue that the benefits are experimental, that there are alternative means of achieving the same goals, and that it may violate the ethical liberal norm of 'do no harm'.[133] In stem cell research, for example,

[126]ibid.
[127]ibid.
[128]ibid.
[129]Gómez-Lobo (n 121).
[130]ibid.
[131]ibid.
[132]ibid.
[133]ibid.

where stem cell transplantation can provide a cure for diseases like Alzheimer's or Parkinson's, the embryo from which the stem cell is harvested has to be destroyed.[134]

In the UN Declaration on Human Cloning, the UN General Assembly called for the prohibition of the application of cloning techniques that may contradict human dignity. Following suit, member states have banned embryonic stem cell research either by ratifying the UN Declaration on Human Cloning or by domestic legislation or policy statements.[135]

5.2. Ethical and moral issues in digital cloning

Although digital cloning raises ethical and moral issues too, it raises issues different from biological human cloning. Digital cloning neither involves inherently physically or medically dangerous procedures to the cloned human child, nor does it harm an embryo, as is the case in embryonic stem cell research. In this sense, digital cloning may not evoke objections from the ethical liberal norm of 'do no harm' in the physical and medical sense. The absence of physical harm in digital cloning makes it easier to accept it as morally right when compared to biological human cloning.[136]

Digital cloning is also easier to justify when coupled with the utilitarian argument that digital cloning produces the greatest good for the greatest number of people for purposes of research and developing AI technology. One may argue that digital cloning enhances human understanding and capacity in the areas of the human mind, behaviour, personality, and emotional intelligence. In this sense, digital cloning seems morally acceptable as long as it remains harmless to humans.

However, digital cloning continues to raise ethical and legal issues surrounding applications that are contrary to human dignity, as embodied in the UN Declaration on Human Cloning. Digital cloning also challenges our concept of morality. The domestic laws of many countries ban inventions that violate culturally and religiously defined concepts of morality and public order. In the EU, for example, the European Patent Convention under Article 53(a) denies the grant of a patent to inventions that breach public order or morality.[137] The European Court of Justice confirmed the need to protect human dignity and integrity, which it deems as fundamental rights.[138]

Whereas the creation of deepfakes may carry some entertainment value for a good number of people, it is not until one thinks of a mindclone that ethical and moral issues that challenge our concept of human dignity become a more serious concern. Mindclones certainly raise ethical and moral questions regarding digital immortality. However, they may be more of a philosophical curiosity. When mindclones are combined with behaviour cloning, however, the creation of individualised digital thought clones that can replicate the thoughts, feelings, personality, decisions, and behaviours of a biological person poses more serious concerns about human dignity. Unlike an avatar, which is a visual or digital representation of a person, but does not replicate the person in

[134]ibid.; Iegor Bakhariev, 'Digital Cloning – A Sci-Fi Dream or a Legal Nightmare?' *Inside Scandinavian Business* (Malmo 20 September 2019) <https://www.insidescandinavianbusiness.com/article.php?id=472> accessed 17 November 2019.
[135]Bakhariev (n 130).
[136]ibid. (noting that the 'health impacts of digital clones are, as of yet, unknown. It is quite possible that such clones might have an impact on psychological health and mental stability').
[137]ibid.
[138]ibid.

entirety, a digital thought clone can actually anticipate and replicate a biological person's actions and decisions.

6. Potential ethical issues raised by cloning in the digital world

Under the umbrella of human dignity and morality, digital cloning raises ethical and legal issues pertaining to (1) consent and privacy, (2) immortality, and (3) the philosophical and legal status of digital clones as humans.

6.1. Consent, privacy, and post-mortem privacy

Digital cloning, regardless of the type, raises issues of consent and privacy violations whenever the data used to create the digital clone are obtained without the informed consent of the owner of the data. The issue only arises when the owner of the data is a human. Data created solely by computers or AI may not raise issues of consent and privacy as long as AI and robots are not deemed to have the same legal rights or philosophical status as persons.

The core issue here is whether the privacy of the person who owns or who is the subject of the data was violated. A person's right to privacy can certainly be waived through their consent. Therefore, whether consent was obtained properly or not depends on whether it was informed consent.

The issue especially raises ethical concerns in mindcloning where data on the thoughts, recollections, feelings, beliefs, attitudes, preferences, and values of a person are used to create mind files. Issues of post-mortem privacy also arise in mindcloning when the cloned person did not consent to the creation of a mindclone, or if the use or conduct of the mindclone exceeds the scope of the consent initially given by the deceased cloned person.

In consumer behaviour and digital thought cloning, the issue is certainly germane as to whether consumers have consented to the use of their data to create digital clones. Even if they gave ownership of the data to a company, an issue is whether the use of such data by the company to create a digital clone was foreseen and therefore consented to by the source of the cloned data. A subsequent issue is whether a digital thought clone can consent on behalf of, or concurrently with, the biological person. The resolution of this issue will be determined largely by the data privacy regime governing the digital clone.

In jurisdictions like the US, with the possible exception of California since the effect of the recent data protection legislation there, data are simply seen as property and devoid of the notions of privacy. In jurisdictions like the EU, the concepts of privacy in data have evolved very differently. Concepts of privacy and consent to the use of data to create digital clones will thus depend on how privacy in data has been conceptualised in a given jurisdiction.

Setting the legal issues aside, digital cloning poses a set of challenges to our ethical concepts of privacy. One issue is whether privacy in a biological human can extend to the digital version, and whether a digital clone holds the right of privacy separate from that of its original. The question is especially important in a digital thought clone that can act and think like a biological person. Within the expanding scope of privacy, an

ethical and legal understanding of when the duties of confidentiality arise will need to be re-examined.

6.2. Digital immortality

The creation of a clone in the digital world raises philosophical and ethical issues related to immortality. There already exists research on the creation of mindclones with the aim of eventually transferring a person's consciousness to a digital clone after their biological death.

Transhumanists, who consider science and technology positive tools that can help humans transcend their biological limitations, believe in and are developing technologies that they hope will extend mortality into the realm of immortality, albeit in the digital and synthetic sense.[139] Some transhumanists like Rothblatt have theorised that mindcloning can result in creating digital immortality,[140] while others believe that mindcloning cannot recreate biological consciousness and therefore cannot lead to immortality.[141]

Regardless of the outcome, the transhumanist effort to transfer consciousness and create digital immortality will require a better understanding of the meaning of consciousness and can lead researchers to a better understanding of what it means to be human. Currently, the scientific understanding of consciousness, previously recognised only as a philosophical inquiry, is in its infancy.[142] We do not have a full understanding of how consciousness arises, yet. The two leading scientific theories on consciousness are the global workspace theory (GWT) and integrated information theory (IIT). GWT explains consciousness as the use of a large part of the cerebral cortex with a recognition process that engages a large part of the brain in an integrated manner.[143] IIT explains consciousness as a process that involves a very high level of integrated information within a system.[144] IIT theorists posit that consciousness can arise in computer systems given the ideal conditions.[145] However, they also point out that computers would have to be designed and built to create ideal conditions that can require substantially more information and feedback integration in order to achieve the high levels required to create consciousness.[146]

Transhumanist efforts to create digital immortality raise important fundamental ethical and moral questions on whether we should even attempt to create digital immortality in the first place, and the challenges that such digital immortality poses to our notions of human dignity and morality. Digital immortality, especially with the transference of consciousness, necessitates philosophical and religious debates about the meaning of an after-life.[147]

[139]Jenny Huberman, 'Immortality Transformed: Mind Cloning, Transhumanism and the Quest for Digital Immortality' (2018) 23 M 50–64.
[140]ibid.
[141]Maciamo Hay, 'Mind uploading won't lead to immortality' *H Plus Magazine* (24 April 2014) <https://hplusmagazine.com/2014/04/24/mind-uploading-wont-lead-to-immortality/> (accessed 7 January 2020).
[142]Oscar Rickett, 'How Far Off Are We from the Digital Clones of 'Black Mirror'?' *Vice* (City 15 January 2018) <https://www.vice.com/en_uk/article/zmq8vy/how-far-off-are-we-from-the-digital-clones-of-black-mirror> accessed 17 November 2019.
[143]ibid.
[144]ibid.
[145]ibid.
[146]ibid.
[147]Bakhariev (n 130).

6.3. Philosophical and legal status of digital clones

Another potential issue is whether digital clones can retain or attain the status of personhood in the legal or philosophical sense.

In the legal sense, mindclones can potentially extend the same legal personhood status of the biological person as the mindclone is a copy and extension of the biological person's thoughts, recollections, feelings, beliefs, attitudes, preferences, and values. Digital thought clones may present an even stronger argument, especially with the consent of the biological person. Can a digital thought clone be deemed a digital agent or a digital signature of the biological original?

An important distinction must be made as to whether the digital clone is legally the same as or different from the biological source. Without the extension of legal personhood, digital clones can attain a separate legal personhood either through legal fiction, or some other device such as being made a trustee of the biological person.[148] Whereas the question is simply hypothetical, different jurisdictions may have different approaches to legal personhood,[149] and the question will add to the ongoing broader discussion as to whether AI can attain legal personhood status.[150]

Regardless of their legal status, digital clones will prompt philosophical questions on whether a digital extension of a person's thoughts, recollections, feelings, beliefs, attitudes, preferences, and values means that the digital clone is the same as the biological version. Boden recognised, in her philosophical inquiry, the possibility of cloned immortality in computers.[151] However, she did not reflect further on the consequences of the digital clone's existence. Taking the literature on the philosophy of the mind and cybernetics into account, Yampolskiy proposed a variant of the Turing test to determine whether the mind is identical to its digital clone.[152] The question of whether the digital clone can be said to have attained consciousness will be relevant to the inquiry, but not necessarily the ultimate determinant. A subsequent inquiry will determine whether the digital clone's consciousness is the same as that of the biological source.[153] The scenario raises the question of whether consciousness can be extended from the biological to the digital. Lacking consciousness, philosophical inquiry may also turn on whether the digital clone can be said to have a will of its own.

7. Conclusion

This article discussed the legal and ethical implications of digital cloning and digital thought clones in particular, raising the need to reconsider existing theoretical frameworks of privacy, including Nissenbaum's contextual integrity theory, to protect against digital thought clones. A human-centred approach is necessary to arrive at a more

[148]Lawrence B. Solum, 'Legal Personhood for Artificial Intelligence' (1992) 70 NCLR 1231 (analysing whether AI can attain legal personhood status as a trustee).
[149]Bakhariev (n 130).
[150]Alexis Dyschkant, 'Legal Personhood: How We Are Getting It Wrong' (2015) UILR 2075.
[151]Margaret Boden, '*AI: Its Nature and Future* (Oxford University Press, 2016).
[152]Roman V Yampolskiy, *Artificial Superintelligence: A Futuristic Approach* (CRC Press, 2015); Roman V Yampolskiy 'The Space of Possible Mind Designs' in J Bieger, B Goertzel and A Potapov (eds), *Artificial General Intelligence* (AGI, 2015).
[153]In the legal personhood of AI literature, the focus is on whether an AI has attained a will or consciousness. A digital clone takes the inquiry further because of the clone's relation to the biological origin. Kosinski (n 20); Solum (n 144); Dyschkant (n 146).

comprehensive regulation that is needed to cover the rise of digital thought clones. An examination of existing data protection laws in the EU and the US, as examples, reveal the gaps in regulating digital thought clones. Finally, the article discusses the ethical and moral challenges raised by digital thought clones.

The use of digital cloning is inevitable because of the digitisation of human processes and activities. Given the advent of AI, which feeds on the processing of data, it is not surprising that we will use it to interpret endless amounts of data on ourselves. When humanity's unquenchable thirst for understanding human behaviour, decision-making, and the human mind are coupled with economic incentives, the idea of a digital thought clone is not surprising. Yet, it is not only about commerce, but also about influencing how we behave, think, and make choices – encompassing political, social, and personal decisions on matters such as health. Digital thought cloning is simply a means of modelling individual humans through the use of AI. Imagine what digital thought cloning can do to prevent a global pandemic – everyone can be plugged into a real-time monitored health diagnosis. When combined with the behaviour and decision data in digital thought clones, we can predict and monitor a pandemic before it even starts to spread.

However, we must not ignore these consequences. The negative misuse of digital thought clones are as tempting as the positive social and economic benefits. To understand these consequences, we must understand the power that digital thought cloning gives to those with access to personal data. Digital thought cloning allows for accurate individualised modelled predictions about what we do, where we go, what we eat, who we interact with, what we prefer, and many other aspects of our personal lives. These powerful insights can unfortunately be used to manipulate our decisions, or to take away our ability to make decisions with harmful or detrimental effects in financial and other terms.

It is important at this early stage in the technology's evolution to consider the ethical and legal implications of digital thought clones. The legal and ethical issues discussed in this article are only proposed starting points. There are certainly more questions that need to be addressed, most of which pertain to ownership and control over data and privacy, and whether data about our lives should remain in our individual control or be traded as a valued commodity.[154]

This article argued for the responsible regulation of data that carefully balances the policy interests of individual choice and privacy against economic and public interests. This means requiring transparency over the use of digital thought clones, and accountability and explicability of AI algorithms that have access to personal data. This means giving people the right to make an informed choice over their data before creating a digital thought clone. While drafting regulations, this article proposes drawing upon a broad view of the various legal and ethical issues raised by digital cloning and digital thought clones.

[154]Zuboff (n 41), stating that 'these prediction products are traded in a new kind of marketplace that I call behavioural futures markets. Surveillance capitalists have grown immensely wealthy from these trading operations, for many companies are willing to lay bets on our future behaviour'; see also Zuboff (n 1); John Naughton, 'The Goal is to Automate us': Welcome to the Age of Surveillance Capitalism', *The Guardian* (London, 20 January 2019(<https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook> (accessed 11 February 2020).

The European Commission is leading the way in regulating data protection and AI. The European Commission's 2020 White Paper[155] on AI aims to create an 'ecosystem of trust' through AI regulation, accompanied by the European Strategy for Data.[156] The strategy seeks to empower European citizens with additional tools to protect and manage their own data,[157] and more importantly, seeks to socialise ownership of non-personal data. By sharing this latter category of industrial data, the Commission hopes to develop a 'genuine single market for data'.[158] Sharing non-personal data would provide opportunities for increased competition and innovation and offer equal opportunities for both start-ups and large enterprises without data monopolisation. The Commission believes that data-sharing can empower citizens to improve their decision-making to their advantage. Their personal data would not be socialised but would be subject to further protection through the strategy.[159]

Disclosure statement

No potential conflict of interest was reported by the author(s).

[155]'White Paper on Artificial Intelligence - A European approach to excellence and trust' Brussels, (City 19 February 2020) <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf>

[156]'Communication from the Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions A European strategy for data' *European Union* (City 19 February 2020) <https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf>.

[157]For example, 'My Data' <https://mydata.org/>.

[158]*European Union* (n 154).

[159]This publication was made possible by the NPRP award NPRP11C-1229-170007 from the Qatar National Research Fund (a member of the Qatar Foundation). The statements made herein are solely the responsibility of the authors. Open Access funding provided by the Qatar National Library.