International Journal of Law and Psychiatry 67 (2019) 101498

Contents lists available at ScienceDirect

International Journal of Law and Psychiatry

journal homepage: www.elsevier.com/locate/ijlawpsy

Mapping the rise of digital mental health technologies: Emerging issues for law and society

Piers Gooding

Melbourne Social Equity Institute & Melbourne Law School, University of Melbourne, 3010, Australia

ABSTRACT

The use of digital technologies in mental health initiatives is expanding, leading to calls for clearer legal and regulatory frameworks. However, gaps in knowledge about the scale and nature of change impede efforts to develop responsible public governance in the early stages of what may be the mass uptake of 'digital mental health technologies'. This article maps established and emerging technologies in the mental health context with an eye to locating major socio-legal issues. The paper discusses various types of technology, including those designed for information sharing, communication, clinical decision support, 'digital therapies', patient and/or population monitoring and control, bio-informatics and personalised medicine, and service user health informatics. The discussion is organised around *domains of use* based on the actors who use the technologies, and those on whom they are used. These actors go beyond mental health service users and practitioners/service providers, and include health and social system or resource managers, data management services, private companies that collect personal data (such as major technology corporations and data brokers), and multiple government agencies and private sector actors across diverse fields of criminal justice, education, and so on. The mapping exercise offers a starting point to better identify cross-cutting legal, ethical and social issues at the convergence of digital technology and contemporary mental health practice.

1. Introduction

It is a truism that technological change makes it possible for people to act in new ways toward each other. Sometimes, as with human organ transfer or genetic sequence 'editing', these actions need to be governed in ways for which there are no precedents. The need for guidance emerges as to how the technology should be permitted, how it can be used responsibly, or when it should be discouraged and even forbidden. The use of digital technologies in the mental health context is beginning to raise these concerns. However, responsible public governance is impeded where the scale of change remains opaque. This article seeks to 'map' new and emerging digital mental health technologies as an essential first step in understanding major implications for legal, social and ethical enquiry.

2. Background

'Digital mental health technology' encompasses multiple technologies and is used here to refer to digital technology *in personalised and/or group mental health initiatives*. Some technologies in this broad category are relatively longstanding, such as online counselling, while others are more recent. Recent examples include psychiatric drugs that have in-built sensors that 'track' ingestion and record medication compliance (Otsuka Pharmaceuticals, 2017), or computational modelling used by social media companies to identify users at risk of self-harm (Rosen, 2017). In criminal law, 'machine learning' has been used to predict the likelihood that a person will offend, including by considering his or her mental health conditions (see e.g., State v. Loomis, 2016), and electronic global positioning systems ('GPS') has been used to 'track' forensic psychiatric patients in several jurisdictions (Miller, 2015). In community-based mental health services in the US, 'Electronic Visit Verification' is being used to log the precise times at which a mental health service home-visit begins and ends (Olowu, 2015). 'Precision psychiatric medicine' has been developed that uses 'big data' to treat individuals based on variability in their genes, environment and lifestyle (Fernandes et al., 2017); electronic mental health records systems have been designed to create 'a record owned by the service user' (Wykes, 2014). The list continues. These few examples suggest a rapid expansion of digital technologies in the mental health context marked by increasing user uptake, clinical application, government investment and industry activity.

For many prominent mental health practitioners, digital technology offers a way to address the 'global mental health treatment gap' (eg Patel et al., 2018). A 40-author report for the World Psychiatric Association's *Commission on the Future of Psychiatry*, for example, claimed that the 'digital psychiatry revolution has arrived' (2017, p. 798). The authors nominated 'digital psychiatry' as a major priority area for future practice, policy and research, which they argued could help 'reach

E-mail address: p.gooding@unimelb.edu.au.

https://doi.org/10.1016/j.ijlp.2019.101498
Received 26 April 2019; Received in revised form 30 July 2019; Accepted 29 August 2019
Available online 15 October 2019

billions of people' (Bhugra et al., 2017, p. 775). With its unconstrained geographic reach and potential to improve the scalability of interventions, 'digital psychiatry' holds potential for 'radical change in… service delivery and the development of new treatments' (Bhugra et al., 2017, p. 775, 803). A 2019 *Lancet Psychiatry* editorial similarly describes a 'general agreement that big data and algorithms will help optimise performance in psychiatry' and Michael Bauer et al. (2019, p. 338) describe the 'widespread agreement by health-care providers, medical associations, industry, and governments that automation using digital technology could improve the delivery and quality of care in psychiatry, and reduce costs'.

Several governments have indeed endorsed digital mental health technology as a cost-effective, accessible alternative or supplement to face-to-face support (see Christensen & Petrie, 2013). In the United Kingdom ('UK'), for example, former Prime Minister Theresa May announced 'a £67.7million digital mental health package' in 2017 (HM Government, 2017). In the US between 2009 and 2015, the National Institute of Mental Health (2017, February) funded $445 million worth of projects concerned with 'technology-enhanced mental health interventions'.

Industry activity mirrors professional and political enthusiasm. 'Health apps' for mobile phones, for example, were valued by some market researchers at US$28 billion in 2018 and were projected to reach US$102.35 billion by 2023 (Knowledge Sourcing Intelligence, 2017). 29% of activity in the health app sector focused on mental health, according to IMS Institute for Healthcare Informatics (2015, p. 6). Indeed, over 10,000 'mental health mobile phone apps' are now reportedly available for download and use (Nicholas, Larsen, Proudfoot, & Christensen, 2015). Some are relatively 'light touch', such as apps that promote lifestyle change and 'wellbeing', while others are more intensive, including apps that effectively transform smartphones into medical devices. 'Digital phenotyping', for example, has been promoted by some clinicians in order to provide 'continuous, passive assessment of behavior, mood, and cognition by applying machine learning to physiological and biometric data gathered by smartphone' (Martinez-Martin, Insel, Dagum, Greely, & Cho, 2018). 'Mindstrong Health', for example, is an app designed to track users' mood and cognition, and identify early signs of depression and other diagnostic categories. *MIT Technology Review* described Mindstrong Health as 'the smartphone app that can tell you're depressed before you know it yourself' (Metz, 2018). (This rhetorical motif, of attributing agency to technologies, recurs throughout the literature). For the estimated five billion people who will be using smartphones by 2025 (Miller, 2012), ubiquitous sensing and digital technologies have the potential to transform responses to emotional/psychological distress *writ large*.

In certain ways, digital mental health technology represents an 'extreme form' of the legal and ethical issues of digital medicine more generally. First, mental health treatment does not necessarily involve physical manipulation of the person by a provider. This difference in care delivery compared to general health has allowed mental health professionals to use forms of communication technology – particularly in online counselling – more so than in other medical fields (Winnike & Dale, 2017, p. 24). Second, digital mental health initiatives often involve increased data sensitivity compared to general health, and greater difficulty and uncertainty in applying legal standards. 'Personal mental health information' is *uniquely sensitive* under current medico-legal frameworks. As with general health, it can help a person access essential health and social services (such as crisis care, early intervention, and welfare services), but unlike most fields in general health, 'personal mental health information' can influence criminal justice proceedings (in attributing culpability, mitigating sentencing, and so on), can attract discrimination (for example, financial and employment discrimination), and perhaps most significantly, can be used to activate state-authorised coercion in the form of hospital detention and forced treatment. In this sense, personal mental health data qualitatively differs from general health data.[1]

In addition, ways of thinking about emotional distress, mental, disorder, disability and so on, have changed greatly in recent decades. Terms like 'mental health initiative' have become more fluid (and contested) in recent decades. Ideas from the field of mental healthcare have expanded into domains outside health services *per se*, including in fields like education, consumer transactions and the criminal justice system—and digital technologies have been incorporated along the way. In education, for example, schools and universities have used machine learning to monitor student data and activate support for students who appear to be in mental health crises (see Castle, 2018). In the consumer context, there is an increase in 'real-time, context-based' insurance, in which consumer behaviour and other factors influence the determination of insurance premiums (Compliance Advocacy Solutions, 2018). The insurance sector has come under particular scrutiny in some countries, for discriminating against persons based on personal mental health information (see e.g. Public Interest Advocacy Centre, 2018). This expansion of 'mental health initiatives' means that any attempt to map digital mental health technologies in the broad sense must look beyond the strict confines of health systems.

The use of digital technologies in the mental health context is not without its discontents. Adrian Guta, Jijian Voronka and Marilou Gagnon (2018, p.62), for example, warn of an emerging 'digital medicine panopticon' that targets 'vulnerable and marginalized communities', including 'people living with HIV, people who use drugs, and people with psychiatric disabilities… whose social location and health behaviours brings them into conflict with medicine, public health, and the law'. The reference to a panopticon – Jeremy Bentham's institutional building and system of control, later popularised by Michel Foucault (1977) as a metaphor for, and analytical concept to examine, the 'modern disciplinary society' – challenges the view that technologies emerge from neutral clinical or technological expertise. Instead, Guta et al. (2018, p.63) insist on viewing at least some digital mental health technologies within a 'larger integrated surveillance apparatus'. Debates between proponents and detractors of digital mental health technologies are likely to accelerate in coming years.

Importantly for this paper, there remains one point of agreement in over-arching debates, and that is that current legal and regulatory structures for digital mental health technologies are inadequate (eg Winnike & Dale, 2017: 23; Duggal, Brindle, & Bagenal, 2018; Parker, Bero, Gillies, Raven, & Grundy, 2019). '[S]erious concerns', for example, were raised in the *Commission on the Future of Psychiatry*, 'regarding the privacy, transparency, and confidentiality of digital health tools' (Bhugra et al., 2017, p. 802). The authors warn of 'commercialised, unproven treatments entering the medical marketplace with detrimental effect' including 'many low-quality and even dangerous apps' (Bhugra et al., 2017, pp. 775, 803). Health and data privacy laws in most countries often omit requirements in relation to digital mental health initiatives. Where requirements do exist, they typically lack detailed regulations or remain 'siloed, with no single sector holding comprehensive oversight' (Parker et al., 2019, p. 168). Some mental health service user groups have raised concerns about data security and privacy, citing fears of discrimination if digitised personal mental health histories were stolen, leaked or sold (see e.g., Gaebler, Toko, Jenkinson, & Wortham, 2018). Clearly, digital technologies can increase the susceptibility of individuals and communities to harms to health and safety, including decreased privacy, third party organisations leveraging information against users' interests, reputational

[1] There may be exceptions to this observation. HIV or infectious diseases, for example, may attract discrimination, stigma, and even lawful, state-based coercive intervention (see Guta et al., 2018). Attempts to clarify categories of digital technologies in the mental health context should not preclude a combined focus with other relevant population groups where issues overlap.

Table 1
Typology: according to function.

Function	Summary
Information Sharing	Health information technology that focusses on information sharing, mainly that of electronic health records.
Communication	Telehealth and 'm-health' (mobile health) which provide a digital interface through which clinical communication can occur, including between clinicians, or between service users and clinicians.
Clinical Decision Support	Ranging from presenting data in a certain way to aid clinicians in their decision making to providing alerts and prompts, to making decisions without clinician input.
Digital Therapies	The use of digital technologies as a treatment, including mobile apps prescribed by doctors.
Patient and/or Population Monitoring, Surveillance and Control	The tracking of individual health information or population health information over time, and the initiatives used to respond to this information, including data analytics used to identify people at risk of certain mental states, and 'digital pills' to monitor medication adherence.
Bio-informatics and Personalised Medicine	The use of technology to understand biological data to be used to inform clinical practice or to personalise care and interventions, such as 'precision psychiatry' and genomic research.
Service User Health Informatics	Technology that supports the actions of the service user within the health system, including personal health records or consumer decision aids.

injury, discrimination, and so on. Multiple laws become relevant, as I will discuss shortly, including laws of civil commitment, consumer privacy, anti-discrimination, criminal law, health law, international human rights law, data protection laws, and laws relating to government surveillance and cybercrime.

Despite this thicket, there is a paucity of scholarship that looks at the broad legal issues arising from digital mental health technology. Legal research that does exist tends to be jurisdiction- and technology-specific. The aim of this paper, therefore, is to 'zoom out' and map the range of emerging digital mental health technologies worldwide. Given this scope, I will discuss the legal issues at a relatively high level of generality.

3. Mapping 'Digital Mental Health Technologies'

One way to categorise digital mental health technologies is according to their *function* (Table 1). Enrico Coiera's (2015) typology of digital health technologies is instructive. Coiera distinguishes between information sharing, communication, clinical decision support, 'digital therapies', patient and/or population monitoring and control, bio-informatics and personalised medicine, and service user health informatics (See Table 1).

Another approach to developing a typology, which I will primarily adopt to structure the remainder of this article, examines *domains of use* according to the users and subjects of various technologies (Table 2). For example, the World Health Organisation (2018) ('WHO') sought to establish a shared language of digital health technologies by distinguishing between four major user categories: (1) clients/service users/patients; (2) service providers; (3) health system management; and (4) data management services. These categories provide a useful starting point for the purposes of this paper. However, the authors of the WHO report explicitly limited their focus to technologies that 'support *health system* needs' and which are '[t]argeted *primarily at public health audiences*' (WHO, 2018, p. 1) (emphasis added). In contrast, my paper is concerned with the use of digital mental health technologies both *within* but also *beyond* health services, as discussed, particularly in contexts such as education, criminal justice and social media. The focus and audience is therefore broader. As such, I have extended the WHO typology as set out in Table 2, and I will draw on Coiera's typology where relevant.

It is outside the scope of this paper to provide an exhaustive list of technologies or a detailed examination of the legal issues they raise in each case. Instead, the intention is to broadly map this expanding field, provide several real-world examples of indicative technologies for each category, and draw out the emerging socio-legal issues.

There may be other relevant categories, and I will refer at the end of the paper to a list of emerging areas of interest, including in areas of forced migration, employment and work, and coercive psychiatric intervention. It is also worth noting that my approach constitutes something of a top-down, institutional analysis, insofar as it focuses on existing, concrete institutions such as health authorities, hospitals networks, education providers, regulatory bodies, and so on. A bottom-up approach might draw on theories of surveillance to frame the issues from a user-centred perspective (see e.g., Galič, Timan, & Koops, 2017).

Table 2
Typology: domains of use.

Who	Summary
Persons seeking support, clients, service users, patients	Used by individuals using services or seeking to gain support for personal mental health matters, including health service users and caregivers, informal supporters, family and so on. Examples include peer group communication, client health records, and citizen reporting of mental health-related issues.
Mental health care providers	Used by people in the health workforce who deliver services. The initiatives would range from referral coordination, clinical decision support, and electronic health records.
Mental health and welfare system co-ordinators	Used in the administration and oversight of health and welfare systems, ranging from managerial actions on supply chain management, human resources, and service auditing, to oversight bodies that monitor the use of secondary personal data. Typical users: healthcare managers and administering bodies, including government agencies and healthcare providers.
Data management services	Used by data management services, which function across systems through the use and management of data. This category includes the technology behind other initiatives, such as the data storage technology behind an electronic health record, or a 'digital pill' that provides a central storage point between the user and her/his clinical treating team.
Criminal justice systems	Used in the criminal justice system and includes GPS surveillance, algorithmic risk-prediction to inform sentencing or disposition, and the sharing of mental health information between criminal justice and other security agencies.
Corporations and businesses that collect personal digital data on consumers	This category includes technology corporations, including insurance or social media companies, that use secondary-use or indirect data that may constitute 'personal mental health information'. Examples include 'AI-based suicide alerts' by social media companies that result in the despatching of police and other first-responders.
Education Providers	Used by education providers. Examples include 'screening' of students, digitisation and storage of student 'mental health data', and so on.

Finally, any taxonomy of digital mental health technologies will be suggestive rather than definitive (Cortez, 2014, p.1190). Technologies that gather data for the purposes of health providers, for example, might be repurposed in the criminal justice system. A 'digital pill' may be a form of 'digital therapy', as well as being a form of monitoring, surveillance and control, and new categories and typologies will emerge. However, despite some fluidity between the categories I have used here, most technologies that are beginning to appear tend to fit primarily within one category or another, offering a useful conceptual heuristic for this exploratory exercise.

3.1. Technologies for people seeking support, clients, service users, persons with psychosocial disabilities, families, and so on

Technologies in this category may include peer group communication, service user-directed personal records, and a variety of self-directed apps and web-programs. Most examples fall into the categories of communication, information sharing and service user health informatics.

Digital decision-making aids, for example, can help facilitate communication and share information between service users and providers, and may help users navigate through services. CommonGround is an example of a computer-interface presented in the waiting rooms of psychiatric medication clinics and other settings 'to support shared decision making in the psychopharmacology consultation' (Deegan, 2007; Deegan, 2010). CommonGround was developed by Patricia Deegan (2007, 2010), who avowedly draws on her experience as a mental health service user. Service users are invited by a peer worker – that is, someone engaged by the service to assist people based on their own lived experience of mental health crisis, mental health service use, and so on – to complete a pre-consultation report about their personal preferences and values before meeting with a medical professional. This may include contextual information, such as the person's aims and values recorded in her/his own words, or her/his preferred activities to promote wellness and recovery (Deegan, 2005; see also, Simmons, Batchelor, Dimopoulos-Bick, & Howe, 2017).

Continuing in the vein of service user health informatives, some digital health records systems now offer service users **'personalised' and 'user-controlled' health records**. The National Health Service ('NHS') *Healthlocker* initiative, for example, uses Microsoft's HealthVault platform to create 'a record owned by the service user' (Wykes, 2014). The system was reportedly developed in collaboration between clinical staff, service users and carers at South London and Maudsley NHS Foundation Trust (2019). The scheme, which remains in a developmental phase at the time of writing, allows service users to write into their medical notes to contextualise diagnoses, plan for crises, record preferences, and see how clinicians use the records. A host of legal and regulatory issues arise concerning data security, privacy, the degree of control a person can exert (can someone delete all or part of their file, for example?), and the role of the record in involuntary interventions under the *Mental Health Act (1983)(England and Wales)*. Within each of these fields of concern, tensions are likely to emerge, as the movement toward 'participatory health' and 'personalisation' intersects with the new possibilities of social and health informatics.

Digital technology can also provide a platform for **peer group communication or 'client to client' communication** facilitated by web-based platforms. Peer-to-peer online support may be particularly valuable in resource limited settings, where support systems may be fragmented and unequally distributed (Naslund et al., 2017); Masood & Niazi, 2018). Peer communication may be facilitated by service providers; for example, in the form of moderated online forums (see e.g., Robinson et al., 2015). However, many virtual groups exist informally. The national Kenyan organisation *USP Kenya (2018)*, p18), for example, operates a virtual support group using the WhatsApp messenger service, which is characterised as being 'fully community-based, operat [ing] outside Kenya's mental health system and [not linked] to any mental health institution'. Many other examples exist, in which peer support, self-support and personal assistance, is offered by digital developers who insist on being non-clinical and non-service affiliated. An emerging array of web-platforms, for example, offer instructions for people wishing to withdraw from prescription psychiatric medications (see e.g., Rebound, 2017), and many are led by laypersons (see Aviv, 2019).[2] There may be legitimate reasons to seek to deprofessionalise and demedicalise some digital platforms, including affirming informal or natural supports, peer supports and so on, as distinct to health-focused interventions – to which any attempt to regulate the space must remain aware. Some research that surveyed the wide range of mental health apps even warned that the field tends to over-medicalise states of distress and may over-emphasise 'individual responsibility for mental well-being' (Parker et al., 2018). Regardless, questions remain about the nature and extent of regulation and legal oversight required for web-based platforms designed for use by individuals seeking support, whether run by services, for-profit businesses, or run informally by advocates. The global reach of such digital technologies – across jurisdictional bounds – adds a further layer of complexity to the legal and regulatory questions that emerge.

As noted, **'mental health apps'** or '**mHealth**' technologies contain dizzying variety, offering tools for self-diagnosis, monitoring, symptom management, treatment, and so on. Most 'mental health apps' seem to be designed for self-directed use by individuals, though some are designed for use by clinicians (Parker et al., 2018). However, the sheer range of apps in the mental health context – again, there are reportedly over 10,000 of them – means that the field contains diverse normative goals, and arguably warrant a typology specific to the field (see e.g. Cortez, 2014). There is considerable research on the legal regulatory implications of 'mental health apps' (see Grundy et al., 2017; Torous & Roberts, 2017a, Torous & Roberts, 2017b; Parker et al., 2019; Parker et al., 2018; Bhugra et al., 2017; Pasquale & Goldstein, 2014). Within this scholarship, there seems to be general agreement that despite the industrial scale of their production, as well as their potential to harm, current regulation is at best unclear and at worst grossly inadequate. These regulatory gaps were highlighted in the UK, for example, when the NHS closed its 'App Library' in 2015 after a study found that 28% of apps lacked a privacy policy (Huckvale, Prieto, Tilney, Benghozi, & Car, 2015; Wicks & Chiauzzi, 2015) and one app even transmitted personal identifiable data that its policy claimed would be anonymous (Wicks & Chiauzzi, 2015). From a regulatory perspective, oversight mechanisms tend to comprise an opaque mix of government regulation, industry self-regulation, and direct education of consumers and practitioners. Foremost concerns in regulatory discussions concerning mHealth are privacy of users and the affirmative promotion of innovation within the sector (Pasquale & Goldstein, 2014, 3). Ethicists raise concerns with mHealth that could apply to many of the technologies discussed throughout this paper, which include matters of: privacy, security and data ownership; the potential for subpoena and government interception (which is greater on digital platforms than most other realms of service engagement); hacking and third-party data ownership; obtaining informed consent; storing and sharing mobile phone data; and equity of access to mHealth technologies (Carter, Liddle, Hall, & Chenery, 2015). Each of these areas raises distinct and sometimes overlapping legal concerns that apply to the broader consequences of 'health information' collection, aggregation and use.

3.2. Mental health care practitioners

Technologies for use by people in the mental health workforce include referral coordination, clinical decision support, and electronic

[2] The Inner Compass Initiative (2019), for example, which provides online resources for tapering off psychiatric medication, states on its website that "[w]e are not a 'mental health' organisation", and instead state that '[w]e are a social-change organisation' whose materials should not be seen 'as medical, mental health, counselling, clinical or professional advice of any kind'.

health records. In the WHO (2018) report noted previously, several subcategories are offered, including: client identification and registration, client health records, healthcare provider decision-support, telemedicine, activity planning and scheduling, and healthcare provider training.

Some forms of clinical decision support are being informed by **'artificial intelligence' and 'machine learning' for use in psychiatric assessment and intervention** (see Bauer et al., 2019; Shatte, Hutchinson, & Teague, 2019). Cynthia Rudin and Berk Ustun (Miller, 2019, Rudin & Ustun, 2018), for example, describe a project that uses a machine-learning algorithm, called 'riskcalibrated supersparse linear integer models' (RiskSLIM) to screen for adult attention deficit hyperactivity disorder in collaboration with a team of psychiatrists. The test reportedly 'allows for a quick, risk-calibrated diagnosis based on the answers to six questions on a self-reported questionnaire' (Rudin & Ustun, 2018, p. 460). Similar efforts have been made to assess the likelihood of a person experiencing psychosis (see Shatte et al., 2019). Adrian Shatte et al.' (2019) scoping study examined the use of machine learning in the mental health context and found that most applications aimed at helping mental health practitioners with detection, diagnosis, prognosis, treatment and support.

Machine learning has also been used in wearable and smart phone technologies to allow for so-called '**digital phenotyping**'. A clinician may record a patient's electronic activities including communications such as email and text messages, metadata about communications, including times and frequencies of communications, broader use behaviour (such as internet browsing, search behaviour), location data, physical mobility, and proximity data (Fisher & Appelbaum, 2017, p. 171). Digital phenotyping is used by clinicians with the aim of creating objective parameters that correlate with diagnostic criteria by using extensive data about a person to refine diagnosis and predict behaviour (Martinez-Martin et al., 2018). (Whether empirical support exists for these claims is less clear). Julien Epps (2019) promotes the monitoring of speech, which he argues can be 'conveniently collected non-invasively and non-intrusively at low cost via smartphone and [which] has attracted research attention as a behavioral signal that is indicative of many psychiatric disorders'. Guessing at the potential reach of the technology, Epps (2019) writes:

> Automatic speech-based assessment systems are likely to be applied to screening of the general population or to the monitoring of mental state within an individual (e.g., in response to treatment), rather than to diagnosis… Many speech feature extraction approaches can run in a fraction of real time on a smartphone processor, or extracted features can be efficiently sent via network to a server to process. Similarly, many machine learning approaches are computationally feasible for smartphone platforms.

Epps' comment highlights some of the ethical and legal assumptions that proponents of digital phenotyping may hold, and the relatively low value some clinical innovators may attribute to issues of privacy, security and data ownership. (The claim that 'screening the general population' via machine listening is 'non-invasive and non-intrusive', for example, is likely to seem an extraordinary claim to privacy regulators). Digital phenotyping appears to fit most clearly in the category of population and patient monitoring/surveillance, though contains elements of communication, clinical decision support and digital therapy.

Technologies in the monitoring category will almost certainly attract more stringent legal and regulatory controls. Consider '**digital pills**', for example. Approved for use in 2017 by the US Food and Drug Administration (2017), and by regulatory bodies in the European Union and China (Otsuka Pharmaceuticals, 2017), the 'digital pill' integrates an electronic sensor into a psychotropic pill. The sensor comprises of copper, magnesium and silicon, and functions like a battery by releasing an electric signal on contact with stomach acid. A patch worn on the skin enables transmission between the sensor and a mobile device, such as a smartphone, which allows for the 'tracking' of medication ingestion. With consent, third party individuals, such as a healthcare team or family, can monitor ingestion schedules through a web-based portal. According to documentation released by the Food and Drug Administration (2017), the product is aimed at 'the treatment of schizophrenia, acute treatment of manic and mixed episodes associated with bipolar I disorder and for use as an add-on treatment for depression in adults'. The key benefit of the technology, according to marketing materials, is to better achieve patient compliance with medication (Otsuka Pharmaceuticals, 2017). For mental health practitioners, the information gleaned from the pills can inform both intervention and prognosis; for example, clinical responses would differ for a person whose condition is worsening despite taking medication as prescribed, and a person who is taking medication intermittently or not at all. The blurring of classificatory boundaries - for example, between patient monitoring and control, communication, and bio-informatics/personalised medicine - highlights the need for responsive legal and regulatory frameworks that can integrate multiple, traditionally distinct domains of regulation and other forms of governance.

For psychologists, a wide range of 'digital therapies' exist, most of which concern cognitive behaviour therapy (Andersson, 2018). According to Christopher Fairburn and Patel (2017), **web- or app-based psychological therapies** tend to make use of behavioural rather than cognitive processes and are often presented as educational programmes delivered in 'lessons' rather than treatments delivered in 'sessions'. Digital versions of psychotherapy include 'acceptance and commitment therapy, behavioural activation, interpersonal psychotherapy, mindfulness interventio(Naslund et al., 2017)ns and problem-solving therapy' (Fairburn & Patel, 2017 p.19). Fairburn and Patel write:

> Like the cognitive behavioural interventions, they vary in the extent to which they retain the strategies and procedures of the original treatment. Truly novel digital treatments are few and far between. Examples include positive cognitive bias modification as a potential treatment for depression, virtual reality-based exposure in the treatment of anxiety disorders and persecutory delusions, and the use of robotic technology to improve social interaction in autism spectrum disorders and dementia. An example of an intervention that is still at the experimental stage is the use of a computer game to block the reconsolidation of intrusive traumatic memories (Fairburn & Patel, 2017 p.19 [citations removed]).

This array of interventions may be blended by incorporating face-to-face engagement, or may involve standalone, automated computer, web-based or app-based programs (see eg Christensen & Petrie, 2013; Griffiths, Farrer, & Christensen, 2010).

So-called '**machine counselors**' have also been used in suicide prevention services, and elsewhere. At the time of writing, a largescale suicide helpline in Australia is trialling a so-called 'virtual or robotic counsellor' as the first point of call for website users (Coggan, 2019). The aim, according the organisation, is to make the service faster and easier to access (Coggan, 2019). Titled 'Claire', the computer program uses 'scripts and conversation prompts on the Suicide Call Back Service, asking multiple questions and answers, to figure what risk level the caller is, and where to direct them on the website' (Coggan, 2019). According to the developers, '[p]hone counselors can only speak to one person at a time whereas Claire can speak to lots of people and provide support to people immediately' (Coggan, 2019). The attribution of agency to the non-human entity 'Claire' – which is recurrent in other areas of digital mental health technologies – is striking. One concern from a legal (and indeed moral) perspective is the risk that responsibility among human actors involved is diffused. Who is responsible if something goes gravely wrong when 'Claire' is 'speaking' to a suicidal website user, and where the duties of the website provider begin and end, are questions that remain unanswered.

The above examples are a small number in an expanding field of digital technologies used by mental health service providers. Other examples include **telehealth and m-health**, which provide a digital

interface through which clinical communication can occur. This area has a relatively developed field of scholarship (for a survey of legal issues in the US, see e.g., Winnike & Dale, 2017). The use of digital technology in **precision psychiatry** in which machine learning is used to understand biological data, which can then inform clinical practice or to personalise care and interventions, is also gaining pace (Fernandes et al., 2017), with emerging attention to regulatory, ethical and legal issue (Foulkes, Soda, Farrell, Giusti-Rodríguez, & Lázaro-Muñoz, 2019).

3.3. Health and welfare system co-ordinators, managers, and monitoring bodies

This category concerns the administration and oversight of health and welfare systems, ranging from managerial concerns with supply chain management and human resources (WHO, 2018, p. 8), to the monitoring of service provision. Notwithstanding some of the additional sensitivities of personal mental health data, the mental health context does not at first glance appear to raise distinct legal issues in this domain compared to the general health or welfare service sector. However, some unique developments that fall into this category are noteworthy.

In the US, the **'Electronic Visit Verification'** (or EVV) scheme appears to fall within this category, particularly for the service provider performance auditing. Section 12006 of the 21st Century Cures Act, 2016, which authorises the practice, states:

> "(A) The term 'electronic visit verification system' means, with respect to personal care services or home health care services, a system under which visits conducted as part of such services are electronically verified with respect to—
>
> (i) the type of service performed;
> (ii) the individual receiving the service;
> (iii) the date of the service;
> (iv) the location of service delivery;
> (v) the individual providing the service; and.
> (vi) the time the service begins and ends. (*21st Century Cures Act 2016,* SEC. 12,006)

Section 12006, which falls under Title XII 'Medicaid Mental Health Coverage', mandates that US states implement the Electronic Visit Verification (or 'EVV') for all Medicaid personal care services and home health services that require an in-home visit by a provider.

On the one hand, EVV has been characterised as an effective strategy to prevent medical fraud and improve the quality of services for clinicians, home health workers and service recipients (Olowu, 2015). By taking a record of service delivery, EVV verifies when and where care assistants provide billable labour and essentially provides a form of audit protection. On the other hand, depending on who uses EVV, and on whom it is used, the practice constitutes service user and/or population monitoring, surveillance and control. Jacob Metcalf (2018) argues that EVV is a 'deceptively intrusive tracking of the lives of Medicaid recipients' using a third-party contractor to manage the check-in process, a 'backend database prone to leaking protected personal health data', and an in-built design that requires onerous administrative labour by the service recipient. He argues that:

> without careful controls and ethical design thinking, surveillance of caregiver labor is also functionally surveillance of care recipients, especially when family members are employed as caregivers. And all evidence points to the likelihood that this surveillance can easily be repurposed as leverage to reduce access to Medicaid. There should be an extremely high burden for requiring technological surveillance as a price for receiving entitlements… When caregivers log into a GPS-enabled EVV device, they also provide a precise and analyzable location history of the clients, and by implication a record of private and Constitutionally-protected behaviour (Metcalf, 2018).

This brief discussion, regardless of the veracity of the claims by proponents and detractors of EVV, highlights how the seemingly neutral, administrative application of digital technology in resource management can raise fundamental legal issues for service users, patients, paid carers/support persons, and citizens who use services. These issues arise amid complex dynamics of state power, and the competing objectives of government agencies and (increasingly privatised) human services. A key legal concern arises as to whether such measures comply with core administrative law standards, such as legality, fairness, transparency and accountability.

Legal questions arising from EVV and other forms of 'welfare surveillance' concern the use of secondary personal data; that is, personal information collected by government agencies or others that was originally collected for another purpose. Finland has made an innovative attempt to improve public governance over the use by government agencies of secondary personal data, including personal mental health data. The Finnish Parliament approved a new general 'Act on the Secondary Use of Social Welfare and Health Care Data' (Laki sosiaali- ja terveystietojen toissijaisesta käytöstä, based on government proposal HE 159/2017) in March 2019 (see Sosiaali- ja terveysministeriö, n.d.). The aim is to ensure flexible and secure use of data by establishing a centralised electronic licence service and a licensing authority for the secondary use of health and social data. The data is dispersed in several information systems managed by different authorities and the new law would clarify regulatory oversight and streamline the processing of data requests, ostensibly allowing faster access to data, improved data security, and clearer application of principles of administrative law, such as improved accountability, transparency, and public participation.

Another area in which health and welfare system co-ordinators, managers or monitoring bodies may employ digital technologies in the mental health context is in the gathering of vital statistics. Lisa Pont and colleagues (Pont, Raban, Jorgensen, Georgiou, & Westbrook, 2018), for example, used new **information technology to monitor medicine use** in 71 residential aged care facilities in Australia, with the aim of identifying systemic problems, such as prescribing errors and medication misuse. One of the authors' major concerns relevant to this paper, was to address the serious rights concerns raised by excessive prescription of psychiatric pharmaceuticals. Their digital initiative used routinely collected date to alert regulators to high rates of psychotropic medication-use in some facilities that could not be easily explained, flagging the need for further checks. Similarly, Johanna Westbrook et al. (2012), produced some evidence to show that **commercial electronic prescribing or 'e-prescribing' systems** could reduce hospital in-patient prescribing error rates, including in a psychiatric ward in a largescale Australia hospital, mainly by reducing the number of incomplete, illegal, or unclear medication orders. From a regulatory perspective, these findings make a case for giving priority to improving the quality and accessibility of the data in electronic systems over investing in stand-alone, resource-intensive auditing processes.

3.4. Data management services

Technologies in this category are used by data management services. Examples include backend technology that supports other interventions, such as the data storage technology behind an electronic health record, or the central storage point between a mental health app user and a healthcare provider.

As with all digital data, the low-cost storage of digital information compared to paper-based storage raises the issue of a proliferation of copies, and an inability to delete or remove information. Fast data transfer means that mistakes are hard to contain, and high connectivity increases the likelihood of unmoderated content and unintended recipients. In the UK, for example, the national database of medical files, the 'Care.data scheme', was shut down in 2016 after it was found to be selling patient data to drug and insurance companies (Temperton, 2016). In Australia, the introduction of a national health records

database entitled, *My Health Record*, was criticised by a national coalition of organisations representing people with mental health conditions, who called for suspension of the scheme over fears of discrimination if people's digital medical histories were compromised (Gaebler et al., 2018; see also McSherry, 2018).

Data management services are typically subject to existing health data protection laws. For example, the previously mentioned *Healthlocker* scheme must comply with multiple fields of regulation and law, including the *Data Protection Act 1988* (UK) (soon to be replaced by the *Data Protection Act 2018* (UK)) as well as the NHS Code of Practice on Confidentiality by the Department of Health (see South London and Maudsley NHS Foundation Trust, 2019). *Healthlocker* files are transmitted by the Trust and powered by the 'Electronic Patient Journey System' (the trust's electronic record system) and any data transfer must be authorised by Data Processors, who must 'act at all times on […] instructions as the Data Controller under the *Data Protection Act 1998'* (UK). In the US, technologies must be compliant with *Health Insurance Portability and Accountability Act 1996* (HIPAA), which the Department of Health and Human Services enforces to protect identifiable health information. HIPAA was extended by the *Health Information Technology for Economic and Clinical Health Act 2009* (HITECH Act). In 2018, the US Department of Health and Human Services (2019) reportedly distributed over $28 million of fines under HIPPA. Similar data protection schemes exist worldwide, all of which will clearly face new challenges as digital mental health technologies expand.

3.5. Criminal justice systems

Relevant application of technology in the criminal justice system, includes: machine learning in risk prediction to inform policing, sentencing or disposition; GPS monitoring of persons under the supervision of forensic mental health services; and data sharing concerning non-criminal mental health-related incidents, such as hospitalisations or suicide attempts.

Electronic monitoring has been presented as an alternative to incarceration and psychiatric detention (Boone, van der Kooij, & Rap, 2017). Electronic monitoring devices can record and regularly transmit data on a person's location, typically via devices fixed to his or her body. Some GPS devices, such as devices affixed to a person's wrist or ankle, can be linked to blood-alcohol monitors (see Scram Systems, n.d.). Legal responses to electronic monitoring in the mental health context vary greatly. Legislation in the Australian jurisdictions of Queensland and South Australia, for example, authorise health services to impose compulsory 'monitoring conditions' on forensic psychiatric patients using electronic GPS devices (Miller, 2015; South Australia Legislative Council, 2013). The Queensland scheme was introduced against the submissions and evidence of medical practitioners (Miller, 2015).[3] In other jurisdictions, such as the United Kingdom, GPS monitoring schemes exist in forensic mental health services but only on a voluntary basis (see e.g., Tully, Cullen, Hearn, & Fahy, 2016) (notwithstanding issues concerning free and informed consent in forensic psychiatric settings). Research on the effect of a voluntary GPS monitoring scheme in the UK reported a major reduction in '[e]pisodes of leave violation… which suggest potential benefits for speed of patient recovery, reduced length of stay, reduced costs and public safety' (Tully et al., 2016, p. 169). In Nova Scotia, Canada, on the other hand, legislators have *prohibited* the electronic monitoring of forensic mental health patients in any form, with lawmakers citing concerns that such monitoring violates human rights (Moulton, 2015). The province commissioned three reports into the clinical and legal issues, and each study indicated that 'there was no support or even speculative support that electronic monitoring would enhance public safety' (Moulton, 2015). The stark disagreements among lawmakers highlights the diverging ethical and legal approaches currently being taken to the electronic surveillance in forensic psychiatric contexts.

Data sharing by criminal justice agencies also raises significant issues in the mental health context. In one striking example in 2017, Canadians with a documented history of suicide attempts or mental health hospitalisations were being refused entry at the US border (Office of the Privacy Commissioner of Canada (2017) see also, Clarke, 2014). The Office of the Privacy Commissioner of Canada found that the Toronto Police Service had released mental health and suicide data to the Canadian Police Information Centre (CPIC). CPIC had then shared the data with the US Department of Homeland Security, which in turn shared it with US Customs and Border Protection. Several Canadians were then deemed inadmissible to the US under the *Immigration and Nationality Act* (US). The Office of the Privacy Commissioner of Canada (2017, para 107) determined that 'both the specific and systemic aspects of the complaints [were] well-founded', meaning that the relevant government institution—in this case the Royal Canadian Mounted Police, which had stewardship of the CPIC—failed to respect the *Privacy Act* rights of the complainant. Legal regulatory responses could vary from regulation after the fact (as was the case where Canada's *Privacy Act* was enforced and the Toronto Police Service changed its data sharing protocol), to a prospective approach in which preventive regulation strictly controls how non-criminal mental health-related information is collected, used and disclosed.

Finally,**digital technology in forensic psychiatric evaluations** are 'now prominent', according to Patricia Recupero and Federic Reamer (Recupero & Reamer, 2018, p. 208), including through the use of computers (online chat, text messaging, and e-mail) and other electronic means (such as smartphones and videoconferencing technology) to deliver services, communicate with patients, manage confidential case records, and access information about patients and third parties. The use of **algorithms in the administration of justice**, including in determining sentencing and considering a person's risk of re-offending, is another area of concern in the literature (see eg Chiao, 2019), though it remains an issue that has not seen substantial in scholarship concerning mental health and disability.

3.6. Technology firms and other businesses that collect personal digital data on consumers

This category concerns corporations, companies and data brokers that monetise the collection and sale of personal data, which could include 'personal mental health information'. Data in this category is principally derived from social media, apps and connected devices. Whereas data management services could be viewed as 'data warehouses', insofar as they store data for use by health or other services, this category may be crudely considered a 'data marketplace'. Phone and app companies, for example, clearly have the capacity to identify when an individual visits mental health or drug and alcohol services. Referring this possibility, Kate Miller (2019, p.(1983)37) has argued that '[t]he feeling of being watched may alone be sufficient to deter people – especially those from marginalised or minority groups – from feeling truly free to exercise their human rights'. People may be reluctant to visit mental health or support services when this information may be sold, for example to insurance companies.

Social media and major technology firms that gather unprecedented reams of personal data also raise concerns regarding consumers who appear to be in profound distress or mental health crisis. Facebook, for example, has expanded its **pattern recognition software to detect users with suicidal intent** (Card, 2018; Rosen, 2017). Mechanisms within the company can then encourage peer-responses from among the

[3] Major issues with the scheme were exposed in the case of *Re CMX* [2014], in which a man detained in the facility, 'CMX', appealed to the Mental Health Court against the monitoring conditions imposed on him. A treating psychiatrist submitted to the court that '[n]ot only did [the electronic monitoring] device add nothing to his clinical management or risk reduction, it had the effect of hindering his rehabilitation' (*Re CMX*, 2014: 42–43).

person's network, but can also alert authorities (Card, 2018; Rosen, 2017). In 2018, Facebook reported that it had worked with first responders on over 1000 'wellness checks' based on 'reports [Facebook] received from [its] proactive detection efforts' (Card, 2018). Facebook provides some public information as to the algorithm it uses (Card, 2018). However there appears to be little detail as to what precisely is meant by a 'wellness check', though an accompanying video consists of interviews with members of a police force who were sent to the location of an apparently distressed individual. There is no research as to the accuracy, scale or effectiveness of the initiative, nor information on what precisely the company does with the information following each apparent crisis. It is notable that individuals to whom the Facebook 'wellness checks' are directed may be subject to coercive interventions under the terms of typical mental health legislation. This possibility seemingly amplifies consent issues as it seems unlikely that most Facebook users are even aware of the fact that their personal data can be used in this way. Twitter is also a platform through which involuntary mental health interventions have been initiated, as Bernadette McSherry (2018) has discussed, raising concerns about user consent and privacy. In the UK in 2014, for example, the charity Samaritans suspended a Twitter app which enabled users to monitor the accounts of another user for distressing messages, following a backlash from privacy campaigners. Thus, there appear to be very few public governance processes currently available to determine substantive norms in relation to social media suicide alert tools, or other such interventions. Mason Marks (2019, p.1) points out that whereas suicide prediction in medical systems occurs within the healthcare system and is governed by laws such as the HIPAA in the US, as well as regulations that protect the safety of human research subjects and general principles of medical ethics, AI-based suicide prediction on social medial platforms 'typically occurs outside the healthcare system where it is almost completely unregulated, and corporations often maintain their prediction methods as proprietary trade secrets'.

Population monitoring technologies in this category provide new scope for **research and public health interventions using machine learning**, again raising legal and ethical issues concerning privacy and data security. The use of artificial intelligence or machine learning by public health researchers or service providers may help identify people at risk of suicide and direct them to relevant support. However, it is not immediately clear what legal and ethical issues are at play, particularly where the original data is collected by a for-profit business in a 'covert' way. As Nicole Martinez-Martin et al. (2018, p. 2) have written: 'The ability to collect and analyze data surreptitiously or to transform material that is voluntarily made available by individuals for their own purposes into data about those individuals' psychological status raises novel issues of accountability and privacy'. Facebook recently blocked insurers that had been using publicly available data about Facebook users to identify 'conscientious' drivers (Vincent, 2016). Should social media operators be obliged to do the same for those seeking sensitive data concerning mental health? Should such data be available for the purposes of certain kinds of research? If so, what types of research, and how should this be determined? Is it a private matter for companies to self-regulate? What are the legal and ethical responsibilities of researchers who use this data?

Some researchers have sought consent to examine individuals' 'digital footprint' to adduce indicators of mental health conditions. Qijin Cheng, Li, Kwok, Zhu, and Yip (2017), for example, undertook a 'text mining and machine learning study' to determine whether computerised language analysis of Chinese social media could help determine an individual's suicide risk and emotional distress. For groups who face marginalisation and and social adversity—for example, young LGBTQI + people, who may be otherwise hard to identify for the purposes of directing resources or identifying need—legal and regulatory protections concerning population monitoring technologies on social media will be particularly important. At least for research purposes, the processes for reconciling public interest in research using social media data with the public interest in proper privacy protection is not clear (see McSherry, 2018).

3.7. Education providers

Systems of primary, secondary and tertiary education are seeing the incorporation of psychiatric and psychological knowledge and its use in digitised systems. The **digitisation of personal mental health data in schools** raises immediate consent and data security concerns. In 2018, a high school in Melbourne, Australia, for example, mistakenly released the personal digital records of hundreds of students, including information about their 'mental health conditions, medications, and learning and behavioural difficulties' (Australian Associated Press, 2018). This example raises the issue of the sensitivity of children and young people's 'mental health information' in the digital age—a strikingly under-examined issue given the rising use of digital mental health initiatives in child and youth mental health services in particular. As with other domains in which data breaches have occurred, it is not clear what standards are likely to apply in tort law when it comes to accountability in stewarding sensitive records, and the compensation due to students when irreversible breaches occur. Regulatory options in this context could include regulating appropriate information flows, introducing robust standards for digitising sensitive information, including the requirement to obtain individual consent to digitise some types of information, and the introduction of professional standards that prohibit the digitising of certain types of personal information altogether.

However, legislatures may go in the opposite direction and instead, ramping up surveillance over individuals with mental health diagnoses and psychosocial disability. In Florida, in the US, for example, the state legislature mandated the collection and digitisation of student mental health data and its distribution through a statewide database for the putative purpose of preventing gun violence. In 2018, the Florida state government authorised a database as part of a school safety bill passed in the wake of a gun massacre at a Florida high school—the *Florida Senate Bill 7026 or the Marjory Stoneman Douglas High School Public Safety Act*. In May 2019, journalists reported that the type of information the state Department of Education was considering included 'more than 2.5 million records related to those who received psychiatric examinations' (Travis, 2019) under the *Florida Mental Health Act of 1971* (Florida Statute 394.451–394.47891[1] [2009 rev.]). The Department was reportedly considering including 'records for over 9 million children in foster care, diagnosis and treatment records for substance abusers… and reports on students who were bullied and harassed because of their race or sexual orientation' (Travis, 2019). The Bill also may require parents, at the time of initial school registration, to disclose if their child has been referred for mental health service (Rado, 2018). This (extreme) example highlights the sensitivity of personal mental health data in relation to the legal doctrine of 'police powers' that underpin mental health legislation, and its potential re-application for the purposes of preventative policing (regardless of the empirical, legal or moral justification for doing so).

4. Emerging areas

Several areas may warrant attention as emerging fields in which digital mental health initiatives are applied. These include:

- **Coercive interventions in the mental health context.** Several examples discussed in this paper raise the possibility of digital interventions being 'done to' people in coercive interventions, including mandatory datasharing of personal mental health information, and GPS surveillance of forensic psychiatric patients. It seems reasonable to expect that digital technologies may be increasingly used, or proposed for use, in coercive psychiatric interventions, particularly where standard service provision is increasingly digitised.

- **Labour and employment.** Many 'workplace wellness programs' now address 'emotional well-being, mental health and financial wellness' (Kohll, 2016). Several commentators have espoused the benefits of improved productivity and employee wellness (eg Jack, 2017), though others have pointed to the absence of empirical evidence of such claims (Song & Baicker, 2019). The collection and use of what may constitute 'personal mental health data' by employers may well raise issues in privacy and employment law. Employers and wellness program data vendors may well be operating in a legal and regulatory greyzone by using these technologies. Questions remain about how long such vendors may contractually keep employees' wellness data and what analytics they are allowed to perform for what (and whose) purposes (Pasquale & Goldstein, 2014, p. 13).
- **Brain-computer interfaces** present a technology functionality that does not appear in Coiera's typology (Table 1). However, such 'neurotechnologies' are being applied experimentally to areas of mental health research such as suicide prediction (Just et al., 2017), and could profoundly alter some core human characteristics, including matters of 'private mental life, individual agency and an understanding of individuals as entities bound by their bodies' (Yuste et al., 2017). The legal implications of this, admittedly speculative and experimental, field of technology would be enormous, with some medical practitioners already calling for the introduction of a right to 'keep neural data private' (Yuste et al., 2017).

These are some of the emerging areas at the intersection of digital innovation and contemporary mental health practice that seem likely to raise serious legal, social and ethical questions, and many more will no doubt emerge.

5. Conclusion

Part of the challenge of discussing the legal issues raised by the wide-ranging technologies discussed in this article is simply that there are so many. At stake in almost all examples are fundamental rights of dignity, liberty, equality and freedom from exploitation, as well as general ethical principles such as transparency, harm minimisation and accountability. Privacy and data security remain ubiquitous concerns across all digital modalities discussed in this paper. Social and political concerns include the potential concentration of power in the field (among technologists, clinicians, researchers and so on), the need for participatory development of technologies, the challenges of internationalism, the potential diminution of human connection in care relationships, increased pressure on service providers in gathering digital materials (which paradoxically, may reduce time for face-to-face engagement), the expanding notion of 'personal mental health information' in the digital age (Fisher & Appelbaum, 2017, p. 170), the risk of overhyping technology without a commensurate evidence base, and broader questions about the expansion of clinical, government and market power into the lives of individuals.

The cursory mapping exercise in this paper is a preliminary step to making sense of the manifold technological change currently underway. Potential next steps include refining a list of major legal and ethical issues, bringing together relevant actors to prioritise concerns, and proposing a suite of legislative and regulatory options that promote responsible public governance over the diverse limbs of this global trend.

Acknowledgements

I am grateful to Mr. Timothy Kariotis for providing research assistance with this paper.

References

21st Century Cures Act (2016). *Public Law 114-255 (United States)*.
Andersson, G. (2018). Internet interventions: Past, present and future. *Internet Interventions, 12*, 181–188. https://doi.org/10.1016/j.invent.2018.03.008.
Australian Associated Press (2018, August 22). *Melbourne student health records posted online in 'appalling' privacy breach*.
Aviv, R. (2019, April 1). The challenge of going off psychiatric drugs. New Yorker. Retrieved from https://www.newyorker.com/magazine/2019/04/08/the-challenge-of-going-off-psychiatric-drugs.
Bauer, M., Monteith, S., Geddes, J., Gitlin, M. J., Grof, P., Whybrow, P. C., & Glenn, T. (2019). Automation to optimise physician treatment of individual patients: Examples in psychiatry. *The Lancet Psychiatry, 6*(4), 338–349.
Bhugra, D., et al. (2017). The WPA-lancet Psychiatry commission on the future of Psychiatry. *The Lancet Psychiatry, 4*(10), 775–818.
Boone, M., van der Kooij, M., & Rap, S. (2017). The highly reintegrative approach of electronic monitoring in the Netherlands. *European Journal of Probation, 9*(1), 46–61. https://doi.org/10.1177/2066220317697660.
Card, C. (2018, September 10). How Facebook AI helps suicide prevention. *Facebook Newsroom*. Retrieved from https://newsroom.fb.com/news/2018/09/inside-feed-suicide-prevention-and-ai/.
Carter, A., Liddle, J., Hall, W., & Chenery, H. (2015). Mobile phones in research and treatment: Ethical guidelines and future directions. *JMIR mHealth and uHealth, 3*(4), e95. https://doi.org/10.2196/mhealth.4538.
Castle, L. (2018). How a UA professor is using data to identify potential dropouts. Retrieved from https://www.azcentral.com/story/news/local/arizona-education/2018/03/26/university-arizona-predict-dropouts-student-id-card-data/420348002/.
Cheng, Q., Li, T. M., Kwok, C.-L., Zhu, T., & Yip, P. S. (2017). Assessing suicide risk and emotional distress in Chinese social media: A text mining and machine learning study. *Journal of Medical Internet Research, 19*(7), https://doi.org/10.2196/jmir.7276.
Chiao, V. (2019). Fairness, accountability and transparency: Notes on algorithmic decision-making in criminal justice. *International Journal of Law in Context, 15*, 126–139.
Christensen, H., & Petrie, K. (2013). State of the e-mental health field in Australia: Where are we now? *The Australian and New Zealand Journal of Psychiatry, 47*(2), 117–120.
Clarke, K. (2014, June 5). *Ontario privacy commissioner initiates legal action against Toronto police for releasing suicide data to U.S.* National Post. Retrieved from https://nationalpost.com/news/toronto/ontario-privacy-commissioner-initiates-legal-action-against-toronto-police-for-releasing-suicide-data-to-u-s.
Coggan, M. (2019, April 4). *Virtual counsellor steps in to help out on suicide hotline.* PBA. Retrieved April 8, 2019, from pro bono Australia website: https://probonoaustralia.com.au/news/2019/04/virtual-counsellor-steps-in-to-help-out-on-suicide-hotline/.
Coiera, E. (2015). *Guide to health informatics.* CRC press.
Compliance Advocacy Solutions (2018, March 4). Re-imaging mental illness & insurance through Insurtech & social purpose. Retrieved April 15, 2019, From website https://complianceadvocacysolutions.com.au/re-imaging-mental-illness-insurance-through-insurtech-social-purpose/.
Cortez, N. (2014). *The Mobile health revolution? 47*, Davis: University of California1173–1230.
Deegan, P. E. (2005). The importance of personal medicine: A qualitative study of resilience in people with psychiatric disabilities. *Scandinavian Journal of Public Health. Supplement, 66*, 29–35.
Deegan, P. E. (2007). The lived experience of using psychiatric medication in the recovery process and a shared decisionmaking program to support it. *Psychiatric Rehabilitation Journal, 31*, 62–69.
Deegan, P. E. (2010). A web application to support recovery and shared decision making in psychiatric medication clinics. *Psychiatric Rehabilitation Journal, 34*, 23–28.
Duggal, R., Brindle, I., & Bagenal, J. (2018). Digital healthcare: Regulating the revolution. *British Medical Journal, 360*, k6.
Epps, J. (2019, June 4). Digital mental health: How to engage with innovation, Part 2. *Psychiatric Times*. Retrieved from: https://www.psychiatrictimes.com/telepsychiatry/digital-mental-health-how-engage-innovation-part-2.
Fairburn, C. G., & Patel, V. (2017). The impact of digital technology on psychological treatments and their dissemination. *Behaviour Research and Therapy, 88*, 19–25. https://doi.org/10.1016/j.brat.2016.08.012.
Fernandes, B. S., Williams, L. M., Steiner, J., Leboyer, M., Carvalho, A. F., & Berk, M. (2017). The new field of 'precision psychiatry. *BMC Medicine, 15*(1), 80. https://doi.org/10.1186/s12916-017-0849-x.
Fisher, C. E., & Appelbaum, P. S. (2017). Beyond googling: The ethics of using Patients' electronic footprints in psychiatric practice. *Harvard Review of Psychiatry, 25*(4), 170–179.
Food and Drug Administration (US) (2017, November 13). *FDA News Release: FDA approves pill with sensor that digitally tracks if patients have ingested their medication, New tool for patients taking Abilify.* Retrieved from: https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm584933.htm>.
Foucault, M. (1977). *Discipline and punish.* New York: Pantheon.
Foulkes, A., Soda, T., Farrell, M., Giusti-Rodríguez, P., & Lázaro-Muñoz, G. (2019). *Legal & amp; Ethical Implications of CRISPR Applications in Psychiatry (SSRN scholarly paper no. ID 3348184).* Retrieved from Social Science Research Network. website https://papers.ssrn.com/abstract=3348184.
Gaebler, S., Toko, M., Jenkinson, S., & Wortham, R. (2018). Joint letter to minister hunt – My health record. Retrieved from http://being.org.au/2018/08/joint-letter-to-minister-hunt-my-health-records/.
Galič, M., Timan, T., & Koops, B.-J. (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the Panopticon to participation. *Philosophy & Technology, 30*(1), 9–37. https://doi.org/10.1007/s13347-016-0219-1.

Griffiths, K. M., Farrer, L., & Christensen, H. (2010). The efficacy of internet interventions for depression and anxiety disorders: A review of randomised controlled trials. *The Medical Journal of Australia, 192*(11 Suppl), S4–11.
Grundy, Q., Parker, L., Raven, M., Gillies, D., Mintzes, B., Jureidini, J., & Bero, L. (2017). *Finding peace of mind: Navigating the marketplace of mental health apps.* Sydney: Australian Communications Consumer Action Network.
Guta, A., Voronka, J., & Gagnon, M. (2018). Resisting the digital medicine Panopticon: Toward a bioethics of the oppressed. *The American Journal of Bioethics, 18*(9), 62–64. https://doi.org/10.1080/15265161.2018.1498936.
HM Government (2017). Press release: Prime minister unveils plans to transform mental health support. www.gov.uk/government/news/prime-minister-unveils-plans-to-transform-mental-health-support.
Huckvale, K., Prieto, J. T., Tilney, M., Benghozi, P., & Car, J. (2015). Unaddressed privacy and security risks in accredited health and wellness apps: lessons from a cross-sectional systematic assessment. *BMC Medicine,* 2015.
IMS Institute for Healthcare Informatics (2015). Patient adoption of mHealth: Use, evidence and remaining barriers to mainstream acceptance. Retrieved from https://www.iqvia.com/-/media/iqvia/pdfs/institute-reports/patient-adoption-of-mhealth.pdf.
Inner Compass Initiative (2019). About inner compass initiative. (website). Retrieved from: https://www.theinnercompass.org/about.
Jack, A. (2017, September 13). Wellness schemes benefit employers as well as staff. *Financial Times*. Retrieved from: https://www.ft.com/content/86edc1b6-371b-11e7-99bd-13beb0903fa3.
Just, M. A., Pan, L., Cherkassky, V. L., McMakin, D. L., Cha, C., Nock, M. K., & Brent, D. (2017). Machine learning of neural representations of suicide and emotion concepts identifies suicidal youth. *Nature Human Behaviour, 1*(12), 911–919. https://doi.org/10.1038/s41562-017-0234-y.
Knowledge Sourcing Intelligence (2017, 24 November). Mobile health (mHealth) app market - industry trends, opportunities and forecasts to 2023. Retrieved from: https://www.wiseguyreports.com/reports/3205042-mobile-health-mhealth-app-market-industry-trends-opportunities.
Kohll, A. (2016, April 16). 8 things you need to know about employee wellness programs. *Forbes*. Retrieved from: www.forbes.com/sites/alankohll/2016/04/21/8-things-youneed-to-know-about-employee-wellness-programs/#1ec78c4d610c.
Marks, M. (2019). Artificial intelligence based suicide prediction – Early draft version. *Yale Journal Health Policy Law & Ethics*. (forthcoming) 36. Electronic copy available at https://ssrn.com/abstract=3324874.
Martinez-Martin, N., Insel, T. R., Dagum, P., Greely, H. T., & Cho, M. K. (2018). Data mining for health: Staking out the ethical territory of digital phenotyping. *Npj Digital Medicine, 1*(1), 68–73.
Masood, M., & Niazi, N. H. (2018, July 5). Digital spaces in Pakistan as alternative care communities. *Mad in Asia*. Retrieved from https://madinasia.org/2018/07/digital-spaces-in-pakistan-as-alternative-care-communities/.
McSherry, B. (2018). Computational modelling, social media and health-related datasets: Consent and privacy issues. *Journal of Law and Medicine, 25*(4), 894–898.
Mental Health Act (1983) (England and Wales)
Metcalf, J. (2018, February 27). When verification is also surveillance. *Data and Society*. Retrieved from: https://points.datasociety.net/when-verification-is-also-surveillance-21edb6c12cc9.
Metz, R. (2018). The smartphone app that can tell you're depressed before you know it yourself. Retrieved July 12, 2019, from MIT Technology Review website: https://www.technologyreview.com/s/612266/the-smartphone-app-that-can-tell-youre-depressed-before-you-know-it-yourself/.
Miller, G. (2012). The smartphone psychology manifesto. *Perspectives on Psychological Science: A Journal of the Association for Psychological Science, 7*(3), 221–237.
Miller, S. (2015). The use of monitoring conditions (GPS tracking devices) re CMX [2014] QMHC 4. *Psychiatry, Psychology and Law, 22*(3), 321–326.
Miller, K. (2019, October). A MATTER OF PERSPECTIVE: Discrimination, bias and inequality in AI. In T. Walsh (Ed.). *CLOSER TO THE MACHINE Technical, social, and legal aspects of AI. Office of the Victorian Information Commissioner*. Retrieved from https://ovic.vic.gov.au/wp-content/uploads/2019/08/closer-to-the-machine-web.pdf.
Moulton, D. (2015). Nova Scotia sets direction on GPS monitoring of patients. *Canadian Medical Association Journal, 187*(8), E232–E233.
Naslund, J. A., Aschbrenner, K. A., Araya, R., Marsch, L. A., Unützer, J., Patel, V., & Bartels, S. J. (2017). Digital technology for treating and preventing mental disorders in low-income and middle-income countries: A narrative review of the literature. *The Lancet. Psychiatry, 4*(6), 486–500. https://doi.org/10.1016/S2215-0366(17)30096-2.
National Institute of Mental Health (2017, February). NIMH technology and the future of mental health treatment. Retrieved from https://www.nimh.nih.gov/health/topics/technology-and-the-future-of-mental-health-treatment/index.shtml#part_152632.
Nicholas, J., Larsen, M. E., Proudfoot, J., & Christensen, H. (2015). Mobile apps for bipolar disorder: A systematic review of features and content quality. *Journal of Medical Internet Research, 17*, e198.
Office of the Privacy Commissioner of Canada (2017, September 21). Disclosure of information about complainant's attempted suicide to US customs and border protection not authorized under the privacy act. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2016-17/pa_20170419_rcmp/.
Olowu, A. (2015). Delivering proof of care at the point of care. How electronic visit verification can benefit clinicians, home health workers and patients. *Health Management Technology, 36*(4), 16.
Otsuka Pharmaceuticals (2017, May). Ostuka and Proteus digital health resubmit application to FDA for first digital medicine. https://www.otsuka-us.com/discover/articles-1033.
Parker, L., Bero, L., Gillies, D., Raven, M., & Grundy, Q. (2019). The "hot potato" of mental health app regulation: A critical case study of the Australian policy arena. *International Journal of Health Policy and Management, x(x),* 1–9.
Parker, L., Bero, L., Gillies, D., Raven, M., Mintzes, B., Jureidini, J., & Grundy, Q. (2018). Mental Health Messages in Prominent Mental Health Apps. *Annals of Family Medicine, 16*(4), 338–342. https://doi.org/10.1370/afm.2260.
Pasquale, F., & Goldstein, M. (2014). *The Future of mHealth: Responding to a Changing Regulatory Landscape*. Paper commissioned as part of the American Association for the Advancement of Science mHealth and law workshops. Retrieved from: https://www.aaas.org/sites/default/files/Pasquale-The%20Future%20of%20mHealth.pdf.
Patel, V., Saxena, S., Lund, C., Thornicroft, G., Baingana, F., Bolton, P., & Unützer, J. (2018). The lancet commission on global mental health and sustainable development. *The Lancet, 392*(10157), 1553–1598.
Pont, L. G., Raban, M. Z., Jorgensen, M. L., Georgiou, A., & Westbrook, J. I. (2018). Leveraging new information technology to monitor medicine use in 71 residential aged care facilities: Variation in polypharmacy and antipsychotic use. *International Journal for Quality in Health Care, 30*(10), 810–816. https://doi.org/10.1093/intqhc/mzy098.
Public Interest Advocacy Centre (2018). Mental health discrimination: calls for life insurers be held to account. Retrieved from www.piac.asn.au/2018/04/10/mental-health-discrimination-calls-for-life-insurers-be-held-to-account/.
Rado, D. (2018, July 11). Stigmatizing kids? New law forces families to disclose student's mental health treatment. Retrieved from: https://www.floridaphoenix.com/2018/07/11/stigmatizing-kids-new-law-forces-families-to-disclose-students-mental-health-treatment/.
Rebound (2017, October 2). danish health tech startup - launching first-of-its-kind mobile app to help people safely manage, taper off prescription medications. retrieved from https://www.prnewswire.com/news-releases/danish-health-tech-startup—launching-first-of-its-kind-mobile-app-to-help-people-safely-manage-taper-off-prescription-medications-300528754.html.
Recupero, P., & Reamer, F. (2018). The internet and forensic ethics. In E. Griffith (Ed.). *Ethics challenges in forensic psychiatry and psychology practice* (pp. 208–222). New York; Chichester, West Sussex: Columbia University Press.
Robinson, J., Hetrick, S., Cox, G., Bendall, S., Yung, A., & Pirkis, J. (2015). The safety and acceptability of delivering an online intervention to secondary students at risk of suicide: Findings from a pilot study. *Early Intervention in Psychiatry, 9*(6), 498–506. https://doi.org/10.1111/eip.12136.
Rosen, G. (2017). Getting our community help in real time. *Facebook Newsroom.*. Retrieved from https://newsroom.fb.com/news/2017/11/getting-our-community-help-in-real-time/.
Rudin, C., & Ustun, B. (2018). Optimized Scoring Systems: Toward Trust in Machine Learning for Healthcare and Criminal Justice. *Interfaces, 48*(5), 449–466. https://doi.org/10.1287/inte.2018.0957.
Scram Systems (n.d). 'Alcohol Monitoring: Scram Cam'. Retrieved from: www.scramsystems.com/products/scram-continuous-alcohol-monitoring/
Shatte, A. B. R., Hutchinson, D. M., & Teague, S. J. (2019). Machine learning in mental health: A scoping review of methods and applications. *Psychological Medicine, 49*, 1426–1448.
Simmons, M. B., Batchelor, S., Dimopoulos-Bick, T., & Howe, D. (2017). The choice project: Peer workers promoting shared decision making at a youth mental health service. *Psychiatric Services, 68*, 764–770.
Song, Z., & Baicker, K. (2019). Effect of a workplace wellness program on employee health and economic outcomes: A randomized clinical trial. *JAMA, 321*(15), 1491–1501. https://doi.org/10.1001/jama.2019.3307.
Sosiaali- ja terveysministeriö (n.d.). Secondary use of health and social data. Retrieved from: https://stm.fi/en/secondary-use-of-health-and-social-data
South Australia Legislative Council (2013). *Parliamentary debates: Official Hansard.* 5789–5790 (5802–3).
South London and Maudsley NHS Foundation Trust (2019). Healthlocker (website). Retrieved from: https://www.healthlocker.uk.
State v. Loomis (2016). *881 N.W.2d 749, 767 (Wis. 2016) (USA)*.
Temperton, J. (2016, July 6). *NHS care.Data scheme closed after years of controversy. Wired UK.* Retrieved from https://www.wired.co.uk/article/care-data-nhs-england-closed.
Torous, J., & Roberts, L. W. (2017a). The ethical use of mobile health technology in clinical psychiatry. *Journal of Nervous and Mental Disease, 205*(1), 4–8.
Torous, J., & Roberts, L. W. (2017b). Needed innovation in digital health and smartphone applications for mental health: Transparency and trust. *JAMA Psychiatry, 74*(5), 437–438.
Travis, S. (2019, July 9). Florida wants to amass reams of data on students' lives. Retrieved from: https://www.sun-sentinel.com/local/broward/parkland/florida-school-shooting/fl-ne-school-shooting-database-deadline-20190709-i4ocsmqeivdmrhpauhyaplg52u-story.html.
Tully, J., Cullen, A. E., Hearn, D., & Fahy, T. (2016). Service evaluation of electronic monitoring (GPS tracking) in a medium secure forensic psychiatry setting. *The Journal of Forensic Psychiatry & Psychology, 27*(2), 169–176.
U.S. Department of Health and Human Services (2019). Resolution agreements (author website). Retrieved from: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.
Vincent, J. (2016). Facebook blocks insurer exploiting user data to find 'conscientious' drivers. The verge. Retrieved from https://www.theverge.com/2016/11/2/13496316/facebook-blocks-car-insurer-from-using-user-data-to-set-insurancerate.
Westbrook, J. I., Reckmann, M., Li, L., Runciman, W. B., Burke, R., Lo, C., & Day, R. O. (2012). Effects of two commercial electronic prescribing systems on prescribing error rates in hospital in-patients: A before and after study. *PLoS Medicine, 9*(1), e1001164. https://doi.org/10.1371/journal.pmed.1001164.
Wicks, P., & Chiauzzi, E. (2015). "Trust but verify" – Five approaches to ensure safe

medical apps. *BMC Medicine, 13*(1), 205–210.
Winnike, A. N., & Dale, B. J. (2017). Rewiring mental health: Legal and regulatory Solutions for the effective implementation of Telepsychiatry and Telemental health care. *Houston Journal of Health Law & Policy, 17*(21), 21–103.
World Health Organization (2018). Classification of digital health interventions v1.0: A shared language to describe the uses of digital technology for health. Retrieved from http://www.who.int/iris/handle/10665/260480.
Wykes, T. (2014, October 13). Myhealthlocker – The new era for digital empowerment in SLaM - NIHR biomedical research. Retrieved from https://www.slam.nhs.uk/6211.aspx.
Yuste, R., Goering, S., Arcas, B. A., Bi, G., Carmena, J. M., Carter, A., & Wolpaw, J. (2017). Four ethical priorities for neurotechnologies and AI. *Nature News, 551*(7679), 159. https://doi.org/10.1038/551159a.
USP Kenya. (2018). The Role of Peer Support in Exercising Legal Capacity. (author). Retrieved from: http://www.uspkenya.org/wp-content/uploads/2018/01/Role-of-Peer-Support-in-Exercising-Legal-Capacity.pdf 2019, September.