Health, Risk & Society

ISSN: 1369-8575 (Print) 1469-8331 (Online) Journal homepage: http://www.tandfonline.com/loi/chrs20

Digitised health, medicine and risk

Deborah Lupton

To cite this article: Deborah Lupton (2016) Digitised health, medicine and risk, Health, Risk & Society, 17:7-8, 473-476, DOI: 10.1080/13698575.2015.1143247

To link to this article: http://dx.doi.org/10.1080/13698575.2015.1143247

Published online: 04 Mar 2016.

Health, Risk & Society, 2015
Vol. 17, Nos. 7–8, 473–476, http://dx.doi.org/10.1080/13698575.2015.1143247

Routledge
Taylor & Francis Group

EDITORIAL

Digitised health, medicine and risk

The domains of medicine and public health have witnessed a rapid expansion of digital technologies over the past decade. While telehealth and telemedicine and patient online discussion forums were introduced in the 1990s in the wake of personal computing and the development of the Internet, the advent of mobile ubiquitous devices, apps and social media networking sites has resulted in a proliferation of opportunities for people to seek out information about health and medicine, share their experiences and collect their own biometric data. Healthcare professionals and public health workers, for their part, can employ digital technologies for professional and patient education and as part of their applied practice (see overviews of the range of technologies available in Lupton, 2014b, 2015).

A prevailing excitement can be discerned in the medical and public health literature and popular media concerning the apparent 'disruptive' or 'revolutionary' potential of digital health technologies. For example, glowing descriptions of the value of 'prescribing' apps to patients, encouraging people to share their experiences on social media and specialised platforms such as PatientsLikeMe, using big data to develop greater insights into patterns of health and illness, sending people with chronic health conditions home with wireless digital devices for self-care, employing 3D-printing technologies to manufacture prostheses or human tissue, educating medical students using iPads and virtual reality software and using wearable devices and apps for health promotion are common in these literatures.

There is no doubt that these technologies offer many possibilities for improving or enhancing healthcare, preventive health and public health. However, most of the wider social implications are often ignored or glossed over in such accounts. Critical approaches from within the social sciences that take a more measured perspective are important – including those that focus on risk.

Researchers in the social science of risk have various perspectives to offer on digital risk society in general (Lupton, 2016) and digital health technologies more specifically. Among other topics, they can seek to identify the socio-economic disadvantage or inequalities that digital health technologies may exacerbate or generate; show how the digital media represent risk discourses (on websites, Wikipedia, online news reports and social media platforms, for example); highlight the ways in which such technologies as apps and other software identify, algorithmically calculate, perform and manage some phenomena as 'health risks'; and uncover the unintended consequences for both laypeople and health professionals of using digital health technologies in healthcare and public health.

This special issue was designed to encourage social researchers' attention on these issues. Eight articles are included from authors addressing a range of issues concerning digitised health, medicine and risk. Several authors concentrate on apps: Samantha Adams and Maartje Niezen write about eCoaches (online health promotion software and related mobile apps) as they are used as part of a Dutch public–private programme, Antonio Maturo and Francesca Setiffi discuss the gamification of risk in weight-loss apps, Gareth Thomas and myself address the representation of risk and commodity consumption in

pregnancy apps and Alison Kenner analyses the content, development and use of asthma apps. In their article, Maggie Mort and colleagues describe their study investigating how members of a north English community responded to two forms of biosensors for health monitoring: home ovulation and direct-to-consumer genetic testing technologies.

The exchange of information on online forums, blogs, social media sites and websites are examined in two articles. Alan Peterson, Casimir MacGregor and Megan Munsie provide an analysis of how social media were employed by patients to advocate for access to stem cell therapies. Sau Wa Mak's article discusses how Hong Kong mothers used social media and websites to learn about, gain support for and defend their infant feeding practices. Both articles emphasise the great importance that such digital media can have in facilitating lay discussion of health risks and in configuring new forms of biosociality and biological citizenship. Finally, the study reported by Michael Savic and colleagues addresses an Australian online screening intervention for alcohol and other drug-related harms. They identify the ways in which this software enacts certain behaviours and people as 'risky'.

All authors here published adopt an approach that recognises apps and other software, as well as hardware such as wireless patient self-care devices and wearable health and fitness trackers as sociocultural artefacts (Lupton, 2014a). Most of the analyses identify the neoliberal 'soft' politics of digital health, in which laypeople are encouraged ('nudged') to engage in practices of self-management and self-care in their own interests, and the victim-blaming that may be part of these discourses.

As a collection, the articles also highlight the sheer volume of detail about very personal and private elements of people's lives, emotions and bodies that contemporary digital technologies can collect: including their alcohol and drug use, physical activity, genomic information, infant feeding and care practices, medical treatments, eating habits, fertility, reproduction and sexual activity. A dominant feature of these technologies is their 'pushiness'; their tendency to use push notifications and warnings tailored to users' personal details for maximum effect. With their data-collecting capacity, these devices and software offer the ability to configure new forms of risk, in concert with novel responsibilities.

One important aspect of risk in relation to digital health that has not been addressed by the articles in the special collection is that relating to how people's often very private and intimate data about their bodies and behaviours have become exploited by others. The sharing economy of new digital media encourages people to upload their personal information to public forums as part of constructing identity and engaging in social relationships (Banning, 2015). However, people lose control of these details once they are uploaded to proprietary apps and platforms, and they become open to use by many different actors and agencies. In the new knowledge economy, personal digital data have become highly valuable for commercial, research, managerial, governmental and fraudulent purposes. A new digital divide has begun to emerge, in which the Internet empires and other large corporations have ownership of people's personal data while the public has limited access to their own data (Andrejevic, 2014; Fuchs, 2014).

Commercial organisations use the data that they gather from people's online transactions and app use to target them with advertising, or sell the data to third parties (Andrejevic, 2014). The use of personal data by third parties is beginning to have significant implications for people's life opportunities. Data mining companies use personal details that they can scrape from digital datasets (including their health and medical details) to construct profiles about people that may be used to limit their access to insurance, credit, employment and social security benefits (Crawford & Schultz, 2014;

Rosenblat, Wikelius, Boyd, Gangadharan, & Yu, 2014). Another risk relates to how certain social groups are excluded from big datasets because they do not engage in the activities that tend to routinely collect personal data via interactions with digital technologies. These groups tend to be already disadvantaged and marginalised, and this may be exacerbated when government and commercial entities rely on digital data to provide services and shape policy (Lerman, 2013).

A further personal data risk relates to data privacy and security. Data breaches and leakages are common in healthcare organisations and developers' archives of personal data, including those generated by health and medical apps (McCarthy, 2013; Wicks & Chiauzzi, 2015). Digital datasets on personal health and medical details have become a target of cyber criminals, who are able to use this information to profit from identify theft and fraud (Ablon, Libicki, & Golay, 2015).

Before his death, the late Ulrich Beck, a key figure in risk sociology, had begun to comment on what he termed 'global digital freedom risk' in the wake of the Snowden revelations of national security agencies' surveillance of their citizens' interactions online and private telephone records (Beck, 2013). This risk, for Beck, involved not only the threat to privacy, and free speech and communication posed by these security agencies but also the Internet empires. He emphasised the fundamental right of citizens to protect the privacy of their personal data. These issues require continuing attention from critical social researchers.

While this special issue has gone a small way towards contributing to the literature on the social dimensions of digitised health, medicine and risk, many other avenues remain open for exploration. Despite the very common use of social media sites such as Facebook, YouTube, Tumblr and Twitter for the communication of health and medical risk, surprisingly little sociological investigation has been undertaken of these sites. Even though there are now well over 100,000 health and medical apps available for both laypeople and healthcare professionals (Jahns, 2014), few social researchers have directed their attention at analysing the content of these apps and identifying how people are using them (or, why they choose *not* to use them). We know little, as yet, about the rationales and decision-making that underpin health policymakers and digital health developers, or the ways in which citizens are using apps and sensors as part of 'citizen science' public health initiatives. Given the rapidly changing environment of digital health, including new technologies such as apps, 3D-printing, sensor-embedded 'smart' objects and physical spaces and the emerging Internet of Things (in which smart objects communicate directly with each other), there is a panoply of potential topics to explore.

References

Ablon, L., Libicki, M., & Golay, A. (2015). *Markets for cybercrime tools and stolen data*. Santa Monica, CA: RAND Corporation.

Andrejevic, M. (2014). The big data divide. *International Journal of Communication*, *8*, 1673–1689.

Banning, M. E. (2015). Shared entanglements – web 2.0, info-liberalism & digital sharing. Information, Communication & Society, *19*(4), 1–15.

Beck, U. (2013). The digital freedom risk: To fragile an acknowledgement. *OpenDemocracy*. Retrieved from https://www.opendemocracy.net/can-europe-make-it/ulrich-beck/digital-freedom-risk-too-fragile-acknowledgment

Crawford, K., & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review*, *55*(1), 93–128.

Fuchs, C. (2014). *Social media: A critical introduction*. London: Sage.

Jahns, R.-G. (2014). The 8 drivers and barriers that will shape the mHealth app market in the next 5 years. *research2guidance*. Retrieved from http://mhealtheconomics.com/the-8-drivers-and-barriers-that-will-shape-the-mhealth-app-market-in-the-next-5-years/

Lerman, J. (2013). Big data and its exclusions. *Standford Law Review Online*. Retrieved from http://www.stanfordlawreview.org/online/privacy-and-big-data/big-data-and-its-exclusions

Lupton, D. (2014a). Apps as artefacts: Towards a critical perspective on mobile health and medical apps. *Societies*, *4*(4), 606–622. doi:10.3390/soc4040606

Lupton, D. (2014b). Critical perspectives on digital health technologies. *Sociology Compass*, *8*(12), 1344–1359. doi:10.1111/soc4.12226

Lupton, D. (2015). Health promotion in the digital era: A critical commentary. *Health Promotion International*, *30*(1), 174–183. doi:10.1093/heapro/dau091

Lupton, D. (2016). Digital risk society. In A. Burgess, A. Alemanno, & J. Zinn (Eds.), *The Routledge handbook of risk studies* (pp. 301–309). London: Routledge.

McCarthy, M. (2013). Experts warn on data security in health and fitness apps. *British Medical Journal*, *347*(f5600). Retrieved from http://www.bmj.com/content/347/bmj.f5600

Rosenblat, A., Wikelius, K., Boyd, D., Gangadharan, S. P., & Yu, C. (2014). Data & civil rights: Health primer. *Data & Society Research Institute*. Retrieved from http://www.datacivilrights.org/pubs/2014-1030/Health.pdf

Wicks, P., & Chiauzzi, E. (2015). 'Trust but verify': five approaches to ensure safe medical apps. *BMC Medicine*, *13*(1), 205. doi:10.1186/s12916-015-0451-z

Deborah Lupton
News & Media Research Centre, Faculty of Arts & Design,
University of Canberra, Canberra, Australia