My Quantified Self, my FitBit and I

The Polymorphic Concept of Health Data and the Sharer's Dilemma

Argyro P. Karanasiou and Sharanjit Kang

Abstract

The rise of wearable tech, namely devices with sensors measuring the user's daily activities and habits seems to be suggesting a paradox in the post-Snowden era: On one hand, it is generally accepted that unauthorised use, storage and processing of the user's private data by the state directly clashes with our fundamental rights for privacy; on the other, the user seems to be keen on self-recording and storing one's own data by willingly using sensors, enabling him to learn more about one's habits, general health status or even personality. In the era of wearable tech we seem to be accepting that measuring data is not a privacy infringement but a self-surveillance exercise in a quest to get to know ourselves better, most acute to exercising one's right to free expression. Yet, how is this addressed in legal terms? The focal point for this paper is to address the nascent phenomenon of users actively partaking in the QS movement by wilfully sharing health related datasets. Part 1 notes the transition from the "right to be let alone" to the right to own one's data as the underlying rational for QS: is it a form of expression regarding a tradable commodity in a free market or a matter of greater public importance? Part 2 dissects the dilemma in sharing health data for public health and/or research purposes exceeding the strict limits of private sphere. The unfortunate case of Google Health, the unconstitutional purchase of Iceland's national datasets by deCODE and the mishap of the Care.data are studied to shed light to the many faces of our Quantified Selves: Is the current legislative approach fit for facilitating the QS movement, as a type of self-expression? The paper critically examines self-measurement technologies from a legal perspective and calls for urgent reforms in self-measured data protection.

My Quantified Self, my FitBit and I: Performing Self-Surveillance Exercises in the Post-Snowden Era

The rise of wearable tech, namely devices with sensors measuring the user's daily activities and habits seems to be suggesting a paradox in the post-Snowden era: On the one hand, it is generally accepted that unauthorised use, storage and processing of the user's private data by the state directly clashes with our

DOI 10.14361/dcs-2016-0109

fundamental rights for privacy; on the other, the user seems to be keen on self-recording and storing one's own data by willingly using sensors, enabling oneself to learn more about general habits, health status or one's own personality. In this sense, it has been suggested that privacy has gradually changed its meaning: in the era of wearable tech we seem to be accepting that measuring data is not a privacy infringement but a self-surveillance exercise, most acute to exercising one's right to freely express oneself. As a result, wearable technology seems to be holding great potential for moving us from the concept of "online surveillance" towards the concept of "sousveillance" (Kurzweil et al. 2013), namely inverse community-based surveillance instead of a state organised act for the public good. In 2003, Mann, Nolan and Wellman published a pioneering study (Mann et al. 2003), whereby it was demonstrated that wearable tech can aid user empowerment and suggest alternative ways of surveillance. Almost twelve years later, it seems that the user is mostly treated as a mere consumer, wanting not to express oneself through the use of wearable tech but simply to get to know himself better (Rettberger 2014).

The focal point of this paper is to establish a broader understanding of the legal right to privacy, identify links and overlapping areas with other fundamental human rights, such as free speech, and explore these within the scope of autonomy-based legal theories. Premised on the hypothesis that privacy in the digital era has a wider reach than a mere entitlement to non-disclosure or identification, the main aim of the paper is to highlight the limited understanding of this right and further demonstrate how this can be problematic, once applied in health-related data. It is therefore intended to critically study here an often overlooked issue: the many faces data can have and how this tends to challenge conventional legal thinking regarding data sharing. To this cause, health-related data furnishes us with a great study case: The polymorphic concept of health data is used in this paper to validate the hypothesis that the legal understanding of privacy is limited and ought to be revised in the digital era. To demonstrate this, the Quantified Self (QS) movement shall serve as a point of departure. Not only is self-monitoring a perfect manifestation of privacy as a right encompassing self-determination but exploring in depth how wearable tech is utilised to monitor one's own data shall further help our understanding of a nascent field of research, which presents a major legal challenge, due to its direct link to health-related data: data sharing. The policy maker is asked to perform a balancing act between privacy *stricto sensu*, and free expression; a redefined legislative framework for regulating health-related data is therefore essential for knowing where to draw the line. Before however this intricate balance is further looked into, it is essential that self-tracking is first explained.

The growing tendency to self-track and quantify has taken off since its start in 2008 when two former *Wired* magazine editors, Gary Wolf and Kevin Kelly, co-founded the "Quantified Self" digital tracking group. The term is now used to describe the mainstream phenomenon of people collecting data as means of recording and analysing their lifestyle (Haddadi/Brown 2014). It is estimated that 60% of US adults are currently tracking their weight, diet and exercise routine (Swan 2013), actively collecting and analysing their data in the context

of their individual experiences (Nafus/Sherman 2014). The QS movement has further led on to some revolutionary ways of peer interaction regarding commonly faced health problems: self-measured data can gain added value and potentially provide answers, once joined in larger datasets with similar pools of data. Unlike data mining, data sharing has always been considered as an activity that has the potential to give back to the community. The 2016 Pew Research Center study on privacy and information sharing (Rainie/Page 2016) found that there are a variety of circumstances under which many people would share personal information or permit surveillance in return for getting something of perceived value. With regard to health related information, data sharing can further promote a major public health goal: preventive medicine. As Swan notes "the individual, now through quantified self-tracking and other low-cost newly-available tools, has the ability to understand his or her own patterns and baseline measures, and obtain early warnings as to when there is variance and what to do about this" (Swan 2012: 95). This further translated into a new concept of citizenship: "bio-citizenship", namely people using their self-measured data to promote science and aid predictive medicine, often to the detriment of their own privacy.

The fact that users willingly buy and use wearable tech to monitor their daily activities and overall performance, mood and/or health does not implicitly amount to complete consent to their loss of privacy. They do however often engage in data sharing for reasons of treatment personalisation and crowd-sourcing medicine solutions to common health issues. According to a 2015 study by the University of Southern California's Annenberg Center for the Digital Future and Bovitz Inc. (2015) online privacy and data sharing is an issue of trust for users older than 35, whereas it appears to be a purely opportunistic matter of an informed trade-off for younger users, at an age between 17 and 35. For the latter it is a form of expression regarding a tradable commodity in a free market of online services, for the former data sharing concerns the traditional concept of privacy, namely the right to decide whether to reveal or not personal information to the public sphere.

This suggests clearly that the concept of privacy seems to have changed in the era of wearable tech, its focus shifted from the right to be left alone (Warren/Brandeis 1890) to a right to "own" one's data, either for its value determining a fair trade-off or for its fundamental nature as a human right, enshrined in the constitution. Alex Pentland's "New Deal on Data" (Pentland 2013: 83; Pentland 2011) describes data as an asset that can be "possessed, owned and disposed of" (2011) – this description, reflects the current trend of enabling the user to be in control of his data transactions. Is then data sharing a mere transactional act, perhaps ruled by contractual obligations delineating a tradable commodity or is this strictly a matter of privacy law? Most importantly, each time the user willingly performs a self-surveillance exercise the legal boundaries between free expression and privacy appear somewhat blurred. Would this then seem to be paradoxically suggesting that users are willing to entrust private entities with their data as long as they are free to decide themselves how to trade? And how would this explain the public outcry after the Snowden revelations?

In the remainder of the paper it is suggested that the truth is neither here, nor there. It would be a fallacy, an oversimplified claim to argue that the use of wearable tech amounts to the user's admittance that his privacy rights no longer exist. What is argued instead is that we seem to be moving towards a greater autonomy-based concept of privacy. This explains well why self-surveillance also implies an act of self-expression. This further explains the consideration of ownership rights over one's data (Purtova 2011). The next section provides an account of data sharing as both an act of self-expression with a high social value as well as a transaction involving tradable commodities. It will be shown that – although frequently literature and jurisprudence has discussed data from a privacy angle – personal health data sharing is often dealt with as a legal paradox. From there on the paper urges for a legal framework supporting the safe and secure dissemination of health related data. The next section seeks to elaborate further how personal data entails certain levels of autonomy; a rationale, which underpins both privacy and free expression. It should therefore be noted that user-generated and self-measured data is somewhat broader than a mere right to non-disclosure of personal information and ought to be understood as a clear manifestation of self-determination.

Data as a Manifestation of Autonomy beyond the Realms of Privacy

Following conventional methodology, it would appropriate at this stage to provide a definition of privacy; yet, there is no common consensus among legal scholars as to what this human right might entail (Parker 1973: 275). As Post notes: "Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair, whether it can be usefully addressed at all." (2001: 2087). Although privacy is indeed an elusive concept to properly define, it is safe to say that the main concern from a legal point of you is to provide regulative principles for managing the status of one's identity within the overlapping spheres of society, market and the state (cf. Kahn 2003: 372). This understanding of privacy as an entitlement to one's personhood can serve as a point of reference but would still not suffice to provide an accurate definition, especially once privacy is considered within the conceptual scope of another ubiquitous and hardly defined area: big data. The latter, not being touched upon by legal scholars until recently, intensifies the problem of adequately defining privacy in the era of big data (cf. Ward/Barker 2013). The most significant part of the debate though is that data can translate to anything from a legal point of view: information, once seen as data can relate to different rights, not necessarily privacy. What is striking though, is the fact that the principle of autonomy seems to be the underpinning rationale in all these cases. This observation is the argumentative basis for this paper. But before this is further expanded upon with regard to health related data sharing and the QS movement, let's take a closer look at this intricate intersection of privacy and free speech as different sides of the same coin: autonomy.

Free speech theorists have long argued that speech should not be merely considered as a means towards societal progress and collective well-being; it constitutes an intrinsic value indispensable to the individual alone (Rosenfeld 2002: 1535), being an integral part of self-fulfilment and self-realisation of the individual's free potential (Schauer 1982: 49). Applied in the context of big data and wearable tech, these theories document well how the major issue at stake is not the traditional concept of privacy but the wider concept of autonomy, further reflecting on the user's ability to develop and exercise one's own rationality as to how and when to share one's data.

The common ground between the right to free speech and privacy with regard to online data is not identified here for the first time. Jane Bambauer (2014) suggests that, inasmuch data privacy laws control communicatory intellectual interactions among users; data in this context could be treated as speech. This however perplexes matters further when it comes to wearable computing and the QS movement. While users have the ability to monitor themselves and build databases of their daily activities, such data is centrally stored beyond the user's control over data. Should this be regarded speech, then this would effectively grant First Amendment protection to data-brokers and various info-mediaries[1], data mining and processing would thus be regarded as expressive conduct to the detriment of the user's autonomy. This scenario would most certainly raise a major constitutional issue, reaching beyond the scope of private sphere, currently reflected in the data protection regime in the EU and the US. Further to this, Seth Kreimer accepts that there seems to be a major overlap between privacy and free speech in data in the sense that whilst data processing can be protected under the First Amendment, there is not always a countervailing privacy interest (Kreimer 2011: 335-409) to limit data processing, mining or storage. This last point highlights well the many faces of personal data, especially when it is health-related: a commodity, which can be very profitable to a handful of players trading datasets, as well as an asset of high societal value.

Alan Westin's work has been influential in linking privacy and autonomy by defining the latter as a right of the individual to define herself for others; privacy in his view, is not merely a matter of disclosure of personal data beyond the private sphere but rather one's right to "information self-determination" (Westin 1967). Westin articulates privacy as the "claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (ibid: 7). This view maintains a broader scope to a mere right to control one's data: it suggests the ability to self-definition. The latter (right to self-definition) fits comfortably with what has already been discussed thus far with regard to the use of wearable tech and big data, the former (right to control) falls short and cannot be properly applied in an online context (Schwartz 1999: 1609-1701; Schwartz/Reidenberg 1996).

1 See for example *Sorrell v. IMS Health Inc.*, No. 10-779 131 S.Ct. 2653 (2011), where the Supreme Court ruled that data mining and pharmaceutical companies exercise their right to free speech under the First Amendment in mining data from clinicians' prescriptions.

The autonomy-based rationale for private data constitutes a paradigmatic shift from the right to be "let alone" (Warren and Brandeis 1890) to a "right to be let to decide alone" how you wish to be defined as an individual. In the context of wearable tech, it becomes apparent that regulation of aggregated data does not balance free speech against privacy but rather aims at defining how liberty-based fundamental rights are to be weighed against the free flow of information for the public (cf. Reidenberg 1999: 1341-1342). In this view, autonomy can be exercised when an individual is presented with choices and makes an informed decision; a concept unfortunately not evident in contemporary data protection regime.

For the time being however, the lawmaker – mostly at a European level – seems to ignore the autonomy argument as a principle underpinning data sharing. The closest legal criterion still in use is consent – this however appears to be narrower than autonomy: A consent-oriented privacy regime unavoidably focuses on the user as a merely passive data subject and not as an active listener/speaker, whose autonomy needs to be guaranteed as a precondition for making informed choices over one's data. The absence of a robust legal framework able to fully protect QS and data sharing has led to a general feeling of fear and mistrust towards processing and storing user-generated health data. The next section examines three cases of health data processing, whereby it is clearly shown that the law is still lagging behind and does not fully perceive nor protect data as an expression of autonomy but regards it a mere tradable commodity.

Trust by Choice: Towards Voluntary Data Heavens

It has so far been contended that privacy seems to have gained a new meaning in the context of the QS movement: the rationale is no longer to keep information secret but to keep a daily log of one's biometric data with a view to learn more about oneself. At the same time, the emergence of various QS communities eager to share and exchange health data for research purposes, adds another dimension to the issue at hand: when shared, data gains added societal value. This, however, does not suggest that data cannot be monetised or be a valuable asset at the same time: the larger the dataset, the more valuable data becomes. At the moment there is a booming industry dealing with storage, processing and mining of health data. Being both a profitable business and a valuable asset for research, health data poses an interesting dilemma: if shared, it is no longer under the user's control; if it remains hidden, research misses out an unprecedented opportunity to significantly contribute to science.

What is suggested here is that data protection should view biometric data within a wider scope of autonomy with a view to maintain the user's autonomy in the era of big data. One of the most significant consequences of the NSA revelations are that the user's trust in the way online communications are handled by the state and the private industry was shaken. The issue of re-establishing trust has been dominating policy making fora ever since: In January 2016, the report entitled "Big Data: A European Survey on Opportunities and Risks on Data

Analytics", commissioned by Vodafone's Institute for Society and Communications (2016), revealed a great gap in trust on how data is being handled online. Under a third of the 8.000 respondents that took part in the survey appear to be convinced that their personal data is being handled in a trustworthy manner: 18 per cent confirmed their trust in telecommunications providers handling data, whereas 43 per cent trust healthcare institutions, 36 per cent trust their employers and 33 per cent trust banks. Trust becomes a delicate matter, especially once health data in particular enters the discussion of big data: the inefficiency of a robust mechanism of protection of such sensitive data plays a key part in the user's absence of trust. The 2015 BMC Medicine report by Wicks and Chiauzzi confirmed this further. Their review of the accredited National Health Service Health Apps Library found "poor and inconsistent implementation of privacy and security, with 28 per cent of apps lacking a privacy policy and one even transmitting personally identifying data the policy claimed would be anonymous" (2015: 205).

The current legal concept of privacy appears to be fairly limited in dealing with this challenge: Health data analytics can be a double edged sword, having a great potential promote science while at the same time posing a great risk to one's privacy. Drawing the right balance between privacy and scientific progress could be a valuable tool towards rebuilding the user's trust as to how his personal data is dealt with online. At the same time, it can hardly be argued that reinstating trust in health data analytics is a task exclusively reserved for either the state or the private sector: both seem to have failed regaining the user's trust online due to the limitations imposed on the user's autonomy. The unfortunate cases of GoogleHealth, Care.data and deCODE's Health Sector Database explored below demonstrate well this point.

Google Health's Unfortunate End: Trust-Building Exercises

In 2008, Google attempted to reach a critical mass of users and interested third parties and offered them the opportunity to self-manage their health information through a summary records platform. After four years of perseverance, the platform was eventually deserted exposing the public's ignorance and lack of interest (cf. Greenhalgh et al. 2010). The official reasons of Google Health failures have never been released and discontinuation in 2011 has since been justified by the lack of participation from its consumers and collaborators[2]. That said, the rejection of Google Health platform signifies that the lack of robust governance and legislative provisions in place to monitor the access and sharing of sensitive data that fuel the anxieties and evidently led to the reluctance in embracing Google Health. A username and password would activate an individual account where participants could enter their health conditions, medications, allergies and lab results and build a personal health records profile.

2 "An update on Google Health and Google PowerMeter", June 24, 2011 (https://googleblog.blogspot.co.uk/2011/06/update-on-google-health-and-google.html).

Medical records and prescriptions from any of Google's partner hospitals and pharmacies could be imported- however, this potentially highlighted another flaw as there were not enough collaborators within the network embracing the platform.

Predominantly, it became clear individuals felt, and arguably still feel, uncomfortable with the idea of a multinational commercial entity accessing personal health records (cf. Spil/Klein 2014). Principally, Google's privacy policy, "We believe that your health information belongs to you, and you should decide how much you share and whom you share it with [...]. We store your information securely and privately"[3] did not offer proportionate procedural safeguards to reassure its users in failing to detail what they meant by 'securely' and 'privately.' Users were given the option to share their health records with third parties friends, family and doctors with the safeguard that they could always see who had access of their information and permission can be revoked at any time. However, the crux was that once permission was revoked it was implausible to monitor and control who had access to the records as Google could not account for any copies made by third parties who were not governed by privacy regulations during the time permission was valid and the websites that had been linked to a personal health records. Therefore, Google claimed not to assume liability for the information. Competitors such as *Microsoft HealthVault* made bold gestures in joining the Coalition for Patient Privacy[4], committing to the seventeen principles for privacy; whereas Google failed to offer the same level of reassurance and relied solely on their website announcements. Further scrutiny of the fine print revealed Google may share the data patients store on Google Health for the purposes of enabling additional features for other Google products (Tanne 2008: 1207-1211). The general consensus was that the benefit to Google Health outweighed any personal benefit the individuals would receive from sharing their data and the lack of trust between the commercial entity and the public inevitably contributed to its downfall.

Ironically, the Google Inc. offering, which on the surface had the advantage of delivering the scalability required, in reality served as a double edged sword as Google did not only fail to achieve the visibility for the platform to gather a substantial following needed to make the project a success; but with a profit making agenda it aroused concerns around the rigidity of the contemporary data protection safeguards in place. The strength of the safeguards that sought to protect the privacy of its consumers in the face of challenge were questioned. Ultimately, there was a lack of confidence in the intentions of Google and suspicion surrounding the possible intentions behind gathering vast amount of health data, stored in central databases.

3 http://hexus.net/ce/news/general/13383-google-health-launches-plans-manage-well-being/.

4 "Coalition for Patient Privacy", June 13, 2015 (https://patientprivacyrights.org/coalition-patient-privacy/).

It is clear Google has not admitted defeat due to the announcement of 2015, introducing Google X[5], the company's plans for developing a new wearable wristband able to detect, monitor and store data such as pulse, heart rhythm and skin temperature. However, the approach is now different: the company will be seeking regulatory approval for its use in medical contexts, i.e. as a medical device prescribed to patients are used in clinical trials. In other words, the business model seems to be moving from mere collection of data in a central database to a peer-to-peer (patient to doctor) architecture, whereby data is treated as a valuable asset that can be freely exchanged to serve scientific research as well as the patients themselves. This venture is added to a long list of similar initiatives: Apple's *Research Kit*[6], allowing the use of iPhones as medical diagnostic devices by the user without the company's direct involvement is another such example. All these business initiatives, share a very similar pattern: instead of merely performing data mining exercises (often without the user's knowledge or consent), they are mostly interested in enabling user empowerment to share one's data in a decentralized manner. In doing so encouraging users to participate would only improve the quality and quantity of data and if willingly shared, reduce the red tape on the use.

The implications for the trust relationship between these corporations and individuals have somewhat become obscure and almost ignored. It seems corporations such as Google are attempting to bypass the hurdle of establishing trust with their users organically and the rationale now to further their means seems to utilize the patient and doctor relationship. Mostly, whether the more user activity enhances the transparency of its use is yet to be identified.

Care.data: A National Failure to Build a Database

Contrary to Google Health, Care.data was a state run project that had no involvement of private actors. In a highly data driven society, the debacle of Care.data in the UK, examined whether it is possible to strike the right balance between encouragement of the biotechnology industry and protection of the genetic history of citizens (Rodriguez et al. 2013: 276). Once again, public concern regarding medical data privacy halted the plans of the National Health Service in the UK to create a centralized health-care database. The legal framework in place offered little guarantees for the data subject's autonomy: the Health and Social Care Act 2012 enabled the creation of a central database amassing all clinicians' records, while third party usage was justified under the pretext of

5 "Google's new wearable tracks vital signs for medicine", June 23, 2015 (http://www.techradar.com/news/wearables/google-s-new-wearable-tracks-vital-signs-for-medicine-1297586).

6 "Apple ResearchKit Turns iPhones Into Medical Diagnostic Devices", March 9, 2015 (http://techcrunch.com/2015/03/09/apple-introduces-researchkit-turning-iphones-into-medical-diagnostic-devices).

pseudonymised HSCIC[7] datasets. This clearly undermined the right of individuals to make their own informed decisions on healthcare matters.

Moreover, the clinician's lack of clarity and understanding on the legal standards of protection (McGraw 2013: 34) could pose significant privacy threats: in the absence of ample restrictions, other commercial organisations outside the pharmaceutical industry could have unethically and unlawfully accessed the database[8]. Despite the fact that the opt-out policy was later reversed by the NHS, the failures of this project were reflected in the mere 29 % of adult population recalling the leaflet[9] and only a total 19 % supporting it[10]. The fears amongst scholars that the lack of commitment the government has shown on protection of rights in the Care.data project may compromise public trust in research remain very much valid. At the time of the writing, extraction of data is taking place in the UK while the UK's national data guardian Fiona Caldicott has been entrusted with the task to evaluate the fair processing testing communications. In the meanwhile, Care.data is currently being redesigned, along with a number of additional digital services that the NHS is building, following a "crowd coursed" model of online patient care. Note for example, the *Friends and Family Test* (FFT), a dataset of people's comments and ratings of local hospitals[11].

The 2014 Royal Statistical Society "Data Manifesto" puts particular stress on the importance of data sharing encouraging the free and open access of the citizens to national datasets. In dissecting the Care.data debacle the three core issues that were posed began with the extraction of personal confidential data: the processing of the personal confidential data and finally the onward of disclosure of data. When the opt-in selection has been made, the consent hurdle immediately is forgone. In contrast; the doctrine of autonomy is impacted when the individuals are deprived of further regulating any third parties utilizing their personal data in any which way. As previously noted in the Google Health case, the absence of transparency, guidelines and best practises for clinicians and provisions for health related data exchange, are once again a great hindrance to data sharing. It becomes apparent the more confined the control an individual has over the sharing and use of their healthcare data; the greater the hindrance to their autonomy. However, as it will be shown in the next case study, restoring trust is not merely an issue of being able to build a database relying on a robust infrastructure.

7 Health and Social Care Information Center.

8 For example, GE Data Visualization uses information based on 7.2 million patient records from GE's proprietary database, 2011 (http://senseable.mit.edu/healthinfoscape/); Cf. http://www3.gehealthcare.co.uk/.

9 "Adults Unaware of NHS Data Plans", February 14, 2014 (http://www.bbc.co.uk/news/health-26187980).

10 "Three in Four GPs Believe Care.data Should be 'Opt In'", February 26, 2014 (http://www.pulsetoday.co.uk/your-practice/practice-topics/it/three-in-four-gps-believe-caredata-should-be-opt-in/20005954.article).

11 For more details see http://www.nhs.uk/NHSEngland/AboutNHSservices/Pages/nhs-friends-and-family-test.aspx.

DeCODE Disaster: Demystifying the De-Identification Myth

Iceland has been described as "the world's greatest genetic laboratory"[12]: the homogeneity of its population means less genetic variation, which offers an ideal environment for geneticists wishing to conduct medical research based on genome sequencing. Decode Genetics Inc., a for-profit American corporation, published in 2015 four papers in Nature Genetics[13], whereby the findings of sequencing genomes of 2,636 Icelanders (almost 1 % of the total population) were presented. In doing so, the company built one of the most impressive and valuable datasets of genomes, able to contribute significantly towards identifying the genetics of common diseases.

DeCODE's efforts however have been met with lot of scepticism and the way to building their database has not been paved with gold: the company, rose from its ashes in 2012, after it had to file for bankruptcy in 2009 due to its questionable business practises and commercial exploitation of the data mined. The initial plan of the company to raise funds from the public by selling shares to their central database containing health information fell apart, when the law allowing for the creation of their database was found unconstitutional. The company was never able to build the database promised for and did not deliver their public offering.

In order to construct its database, deCODE proposed to collect data from medical records via publicly accessible genealogies, hospitals and health centres and finally from research for which a form of consent was required to be compiled into a *Health Sector Database*[14] The Act on a Health Sector Database (No. 139/1998) was passed by the Icelandic Parliament on December 17th, 1998, after extensive debates in the Parliament and the society at large. The Bill was heavily criticized on numerous counts, including that it lacked provisions for obtaining informed consent of individuals whose information was included in the database, undermined scientific freedom, restrained competition, eroded the doctor-patient confidential relationship, and invaded individuals' right to privacy (Adalsteinsson 2003: 203; Andor 2003: 204). Soon afterwards, DeCODE went into an agreement with the Icelandic State to pay an annual fee in return for being granted a 12 year exclusive license for operating the HSD.

In 2003, the Iceland Supreme Court's Gubmundsdottir v. Iceland,[15] held the compilation of personal health records and available genetic information in one electronic database unconstitutional, unless each individual specifically indicated

12 "Why Iceland Is the World's Greatest Genetic Laboratory", March 25, 2015 (http://www.wired.com/2015/03/iceland-worlds-greatest-genetic-laboratory/).

13 "deCODE Publishes Largest Human Genome Population Study", March 25, 2015 (http://www.bio-itworld.com/2015/3/25/decode-publishes-largest-human-genome-population-study.html).

14 From this point on referred to as HSD.

15 No. 151/2003, Part IV.

otherwise in a pre-defined six-month window unlawful.[16] The database was to include information on children, deceased persons, and incompetent individuals, all of whom are unable to legally provide informed consent to the use of their personal information. The Icelandic Supreme Court[17] held that the HSD Bill did not grant a proportionately adequate protection to the information it was set to contain as demanded by the sensitivity of the information.

The fact that genetic information may reveal medical information not only pertaining to the subject herself but also to relatives was used to argue that genetic information is different and more intrusive than other forms of traditional medical information. In its analysis of the HSD Act, the Icelandic Supreme Court found additional flaws with the Act's protection mechanisms of personal privacy; concluding that the one-way coding mechanism established by the HSD Act is insufficient for protecting individuals' privacy. The Supreme Court's reasoning was two-fold: first, the Act provided no specific guidance as to what type of information must be encrypted in this manner; and second, the Court interpreted the license to imply that after the deletion of an individuals' name and address only personal identification number needed to be encrypted. In effect, although records were be 'de-identified' by removing the name and address and replacing with encrypting the social security number, the encryption done outside control of Roche, they would be linked to genetic, family data. As a result identification would be very easy, given that Iceland would provide a tight context for the data under review- Iceland easy to identify. The Act presumed the consent of patients to release their records to deCODE. Individuals thus must affirmatively opt out in order to prevent their data from being recorded in the health sector database[18] (cf. Árnason 2007).

Predominately, deCODE aspired to rely on theoretical protection of de-identification to reap the benefits of analytics, meanwhile avoiding denunciation for breaching individual privacy. The "silver bullet," (Tene/Polonetsky 2012: 257) of pseudonymisation, anonymisation, encryption and various forms of key-coding was relied on by deCODE to distance data from personal identities in order to justify the secondary uses of personal data. There seems to be a presumption that de-identification and anonymisation renders identification impossible (Ohm 2010: 270). However, it needs to be reiterated that it takes only 33 bits of information to identify a human[19]. The practical problems of medical data allows for linking episodes into longitudinal records, most patients can be re-identified through the 'Incremental Effect' (Narayanan/Shmatikov 2008: 119), where any

16 The HSD Act provided a six-month grace period beginning with the passage of the Act, in which people could choose to opt-out of the project. HSD Act, supra note 11, art. 8. See also infra section IV.A.3.

17 ibid. 5

18 Cf. "Iceland's Research Resources: The Health Sector Database, Genealogy Databases, and Biobanks", NIH Paper, June 1, 2014 (http://grants.nih.gov/grants/icelandic_research.pdf).

19 Cf. "The End of Anonymous Data and What to Do about It", 33 Bits of Entropy, February 5, 2016 (http://33bits.org/about/).

piece of data that has been linked to a person's real identity breaks anonymity and is irreversible. However, New Zealand, demonstrates such a database can effectively exist only when a small number of health service statisticians are permitted to access limited enquiry results of up to six patients at a time in the National Medical Data Set (Neame 1997: 225). The encrypted social security numbers are not considered alone an adequate inference security; (Anderson 1998: 4; Denning 1983; Information/Privacy Commissioner, Ontario, Canada, and Registratiekammer: 1995) special administrative measures are appointed through regulation and data protection legislation with independent government agencies for protection.

It was not until several years later, in 2015, that deCODE (whole owned and operated by Amgen) managed to accumulate genetic data of almost half of the Icelandic population and thus be able to identify people at risk of potential developing a genetic disease. Having failed at receiving legal approval to mine data without consent, deCODE built a research database using clinical data of a large sample of volunteers. If there are any lessons to be learned from deCODE's mishaps is that open data – when addressed as from the perspective of the user and not merely mined and stored into a centralised database – can be of particular significance for advancing scientific research. De-anonymisation and consent have been proven to be the first point of action when lawmakers are faced with health related data mining; yet, how effective are they for protecting the data subject's privacy? Most importantly: at what cost? It is therefore imperative that we further consider the impediment to scientific progress, especially when voluntary schemes of open data exchange can pave the way towards a new system of collecting health related data for national databases.

The next section dissects the issue of monetisation of personal data and seeks to explain how a narrow concept of privacy will not only restore the user's trust but can further pose a significant threat to the QS movement and open data.

Sharing is Caring? The Monetisation of Health Data and the Sharer's Dilemma

The unfortunate cases of online data repositories discussed, highlight that health related data, once perceived as a tradable commodity, poses a significant challenge for privacy scholars: it is no longer one's privacy that is at stake but the user's ability to determine the flow of his personal data. As noted above, autonomy has been identified by legal scholars as one of the underpinning rationales for privacy as well as free speech. It can further be argued that not allowing the user to maintain a certain level of "informational autonomy", namely the ability to control one's personal data flow, can be detrimental to his privacy and undermine any benefits that health data analytics might have.[20] The

20 "Privacy and data protection laws are premised on individual control over information and on principles such as data minimization and purpose limitation. Yet it is not clear that minimizing information collection is always a practical approach

QS movement are a clear manifestation of how the user's autonomy ought to be the basis of a robust data protection legislative framework.

In the early days of wearable tech, user empowerment was the main objective for building an interconnected environment of things and sensors, able to facilitate the needs of the consumer in an automated manner. In 1998 Mann observed: "The most fundamental issue in WearComp [wearable computing] is no doubt that of personal empowerment through its ability to equip the individual with a personalised, customisable operation space owned, operated and controlled by the wearer" (Mann 1998: 2128). Since then, wearable technology has proven to be a profitable business, an industry expected to reach $11.61 billion in revenues by the end of 2020 (Markets and Markets Report 2015). As a result, data is not simply a private or public matter but also a commercial product; a tradable commodity that is part of the daily transactions of several info-mediaries and data-brokers. The recent FTC[21] report from May 2014 "Data Brokers: A Call for Transparency and Accountability" urges the Congress to enhance transparency and user's control over their data (FTC 2014)[22]. That said, instead of user empowerment, the current legislative framework appears to disregard the concept of autonomy. On the other side of the Atlantic, a series of recently leaked proposals (February 2015) for data protection implementation, show that Member States are determined to carve out major guarantees for online privacy offered in the European Commission's proposal for the purposes of an "overriding public interest" (recital 30) or for "scientific purposes". In fact, the leaked documents go as far as re-introducing profiling (originally deleted after the European Parliament's approved text of the proposal in 2014) as an accepted limitation to privacy on grounds of national security, defence, public security and even "other important objectives of general public interest"[23]. This can be an alarming prospect once examined within the context of wearable tech: as noted in the 2015 Nuffield Council on Bioethics report "the bulwarks that have hitherto protected a satisfactory and workable accommodation of interests, principally, the de-identification of data and the 'informed' consent of data 'subjects', have been substantially weakened in a hyper-connected (or potentially hyper-connectable) 'big data' world" (Report of the Nuffield Council on Bioethics 2015).

to privacy in the age of big data. The principles of privacy and data protection must be balanced against additional societal values such as public health, national security and law enforcement, environmental protection, and economic efficiency. A coherent framework would be based on a risk matrix, taking into account the value of different uses of data against the potential risks to individual autonomy and privacy." (Tene/Polonetsky 2012: 67)

21 Federal Trade Commission, hereafter referred to as FTC.

22 FTC (2015): "Data Brokers: A Call for Transparency and Accountability", May 1, 2014 (https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf).

23 For a detailed analysis on the leaked documents see EDRi/Access/Panoptykon/Foundation/Privacy International (2015).

The importance of this in the case of wearable tech and QS is evident once we consider the merits of open data for epidemiology (cf. Barrett et al. 2013): open data in the public domain seems to be gaining some ground in the US and the UK (Business, Innovation and Skills Committee 3rd special report 2013). At the same time though, centralisation is identified as the main obstacle for protecting the user's privacy, carrying the danger of data abuses. This is clearly evidenced in the 2015 Nuffield Report, which states:

"Whereas standardisation is desirable and technical interoperability essential for linking separately collected and maintained datasets, the drive towards exploitation of public data in the UK has, additionally, involved the consolidation and centralisation of some data resources in so-called 'safe havens' for health and public sector data. [...] Although centralisation is convenient for the extraction of value through the application of data analysis, consolidated databases create large targets for unauthorised technical access, unauthorised access by insiders, or abuse of authorised access at the behest of powerful lobbyists" (Report of the Nuffield Council on Bioethics 2015).

The Road Ahead: Quantified Selves and Data Protection Policies

The QS movement and the numerous cases of users wilfully sharing data amongst various online fora, show that data sharing is clearly an act of self-expression, which is in need of robust legal protection: de-anonymisation and consent do not help the users to regain trust but appear to be limited measures offering little protection to open data initiatives.

Unfortunately, the current data protection regime appears to be fragmented and distanced from the notion of autonomy. On one hand the US approach to privacy has been market dominated, reflecting a policy oriented towards treating privacy under consumer rights (Reidenberg 1999). On the other, EU policy for data protection, although reflecting at large a rights-based approach, seems most preoccupied with the enforcement of its regulation in the cloud for strengthening national commercial interests and less concerned with maintaining the user's autonomy as such. According to the Data Protection Directive, a company may process private information on the basis of consent of the user (data subject). Article 29 Working Party has further described that consent is required to be freely given, implicitly and most importantly informed (Opinion 15/2011 on the Definition of Consent 2011: WP187). An informed consent although by definition presupposes a certain level of autonomy to reach a decision, is not easy to grant or legally assess when discussing the use of ubiquitous technologies. In its 2014 report the Working Party has expressed concerns over the problematic applicability of consent within the remit of wearable tech: The fact that an automated system prioritises the ease of a seamless system over constantly informing the user about how his data is collected and processed can further pose a significant barrier to demonstrating valid consent under EU law, as the data subject must be informed" (Opinion 8/2014 on the Recent Developments on the Internet of Things 2014: WP223). Is this a structural deficiency of the

networked environment or an unprecedented legal challenge? It seems that the truth is neither here nor there: the rapid centralisation of datasets, evident in the case studies mentioned above, when combined with a limited range of choices for the user to control processing of his data lies at the heart of the problem.

This paper has sought to explain how boosting the user's autonomy should be the focal point of data protection. The QS movement is a tangible proof of how users are keen to build own datasets and be part of the data processing cycle, joining state and private entities. In this vein, the need for interoperability (Palfrey/Gasser 2012) and data portability is evident. There seems to be a growing interest in data portability in the EU, namely the user's ability to transfer her own data across platforms. This has now been included in article 15 of the Commission's revised proposal[24], which provides that where personal data is processed by electronic means, the user has the right to obtain a copy of their personal data in a "commonly used", "electronic and interoperable" format. Although the concept of interoperability in general is associated at large with copyright law and perhaps appears loosely linked to data protection, its importance for human rights in the digital era can be best demonstrated through the potential it holds for restoring autonomy in online communications.

This last point, arguing for a user-centric internet, seems to be not only supporting an autonomy-based policy model for free speech but for other rights as well, such as privacy. There seems to be a growing tendency to exploit the internet architecture for allowing the user the right to be in sole control of his data shared online, be it speech or personal data. Take for example the concept of privacy by design[25], namely the adoption of privacy enhancing technologies in engineering systems, set out by the Information & Privacy Commissioner of Ontario, Canada, Ann Cavoukian[26] since the early 1990s. Or consider the latest MIT media lab's venture (cf. De Montjoye et al. 2014) open PDS (Personal Data Store): a system that stores data in a repository controlled by the end user, not the application developer or service provider.

The three case studies explored in this paper demonstrate further how data in itself is thus either a valuable tool or a potential threat to the user's fundamental rights. What is suggested here is a positive rights-based approach to maintain a decentralised encrypted networked environment, able to guarantee a certain level of autonomy for the user. Instead of focusing narrowly on protecting one's privacy at the expense of informational flow and free expres-

24 European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

25 "Privacy-Enhancing Technologies: The Path to Anonymity", Information/Privacy Commissioner, Ontario, Canada, and Registratiekammer, The Netherlands, August 2, 1995 (https://www.ipc.on.ca/images/Resources/anoni-v2.pdf).

26 "Cavoukian's Seven Foundational Principles of the Concept of Privacy by Design", March 3, 2015 (http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf).

sion, it is imperative to look at the matter in a contextualised positive manner towards boosting autonomy through a user-centric networked environment.

Acknowledgements

We wish to thank the editors and the anonymous reviewers for all the comments provided. All errors and omissions remain the sole responsibility of the authors.

References

Adalsteinsson, Ragnar (2003): "Human Genetic Databases and Liberty." In: The Juridical Review 2004/1, pp. 65-74.

Anderson, Ross (1998): "The DeCODE Proposal for an Icelandic Health Database". In: Lœknabladhidh (the Icelandic Medical Journal) 84/11, pp. 874-875.

Árnason, Garðar (2007): "Icelandic Biobank. A Report for GenBenefit" (www.uclan.ac.uk/genbenefit).

Article 29 Working Party, Opinion 15/2011 on the Definition of Consent (WP 187), 13 July 2011.

Article 29 Working Party. Opinion 8/2014 on the Recent Developments on the Internet of Things (WP223), 16 September 2014.

Bambauer, Jane R. (2014): "Is Data Speech?" In: Stanford Law Review 66, pp. 65-120.

Barrett, Meredith A./Humblet, Olivier/Hiatt, Robert A./Adler, Nancy E. (2013): "Big Data and Disease Prevention: From Quantified Self to Quantified Communities." In: Big Data 1/3, pp. 168-175.

Business, Innovation and Skills Committee 3rd special report (2013): "Open Access: Responses to the Committee's Fifth Report", March 3, 2013 (http://www.publications.parliament.uk/pa/cm201314/cmselect/cmbis/833/83302.htm).

De Montjoye, Yves-Alexandre/Shmueli, Erez/Wang, Samuel S./Pentland, Alex (2014): "OpenPDS: Protecting the Privacy of Metadata through SafeAnswers." In: PLoS ONE 9/7, pp. e98790.

Denning, Dorothy (1983):"Cryptography and Data Security", Boston: Addison-Wesley.

FTC (2015): "Data Brokers: A Call for Transparency and Accountability", May 1, 2014 (https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf).

Greenhalgh, Trisha/Stramer, Katja/Bratan, Tanja/Byrne, Emma/Russell, Jill/Potts, Henry W. (2010): "Adoption and Non-Adoption of a Shared Electronic Summary Record in England: a Mixed-Method Case Study." In: BMJ, n. p.

Haddadi, Hamed/Brown, Ian (2014): "Quantified Self and the Privacy Challenge", SCL Technology Law Futures Forum, August 2014 (http://www.eecs.qmul.ac.uk/~hamed/papers/qselfprivacy2014.pdf).

Kahn, Jonathan D. (2003): "Privacy as a Legal Principle of Identity Maintenance." In: Seton Hall Law Review 33/2, pp. 371-410.

Kreimer, Seth F. (2011): "Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record." In: University of Pennsylvania Law Review 159/2, pp. 335-409.

Kurzweil, Ray/Minsky, Marvin/Mann, Steve/Bell, Gordon/Nissenbaum, Helen (2013): "The Society of Intelligent Veillance." In: IEEE International Symposium on Technology and Society: Social Implications of Wearable Computers and Augmented Reality in Everyday Life, June 2013, Ontario, Canada.

Mann, Steve (1998): "Humanistic Computing: 'WearComp' as a New Framework and Application for Intelligent Signal Processing." In: Proceedings of the IEEE 86/11, pp. 2123-2151.

Mann, Steve/Nolan, Jason/Wellman, Berry (2003): "Sousveillance: Inventing and Using Wearable Computing Devices." In: Surveillance & Society 1/3, pp. 331-335.

Markets and Markets Report (2015): "Wearable Electronics and Technology Market by Applications (Consumer, Healthcare, Enterprise), Products (Eyewear, Wristwear, Footwear), Form Factors and Geography – Analysis & Forecast to 2014 – 2020", March 3, 2015 (http://www.marketsandmarkets.com/Market-Reports/wearable-electronics-market-983.html).

McGraw, Deven, (2013): "Building Public Trust in Uses of Health Insurance Portability and Accountability Act de-identified Data." In: Journal of the American Medical Informatics Association 20/1, pp. 29-34.

Nafus, Dawn/Sherman, Jamie (2014): "Big Data, Big Questions. This One Does Not Go Up To 11: The Quantified Self Movement as an Alternative Big Data Practice." In: International Journal of Communication 8, pp. 1784-1794.

Narayanan, Arvind/Shmatikov, Vitaly (2008): "Robust de-anonymization of Large Sparse Datasets." In: IEEE Symposium on Security and Privacy, pp. 111-125.

Neame, Roderick (1997): "Smart Cards-the Key to Trustworthy Health Information Systems" In: BMJ 314/7080, p. 573.

Ohm, Paul (2010): "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." In: UCLA Law Review 57, p. 1701-1777.

Palfrey, John/Gasser, Urs (2012): Interop: The promise and perils of highly interconnected systems, New York: Basic Books.

Parker, Richard B. (1973): "A Definition of Privacy." In: Rutgers Law Review 27/2, pp. 275-296.

Pentland, Alex (2011): "Personal Data: The Emergence of a New Asset Class." In: WEF Report (http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf).

Pentland, Alex (2013): "The Data Driven Society." In: Scientific American 309/4, pp. 78-83.

Post, Robert (2001): "Three Concepts of Privacy." In: Georgetown Law Journal 89, pp. 2087-2098.

Purtova, Nadezhda (2011): Property Rights in Personal Data: A European Perspective, Alphen aan den Rijn: Wolters Kluwer.

Rainie, Lee/Duggan, Maeve (2015): "Privacy and Information Sharing", Pew Research Center (http://www.pewinternet.org/2016/01/14/2016/Privacy-and-Information-Sharing/).

Reidenberg, Joel (1999): "Resolving Conflicting International Data Privacy Rules in Cyberspace." In: Stanford Law Review 52, pp. 1315-1371.

EDRi/Access/Panoptykon Foundation/Privacy International (2015): "Data Protection: Broken Badly", Report by Access, EDRi, Panoptykon Foundation and Privacy International, March 3, 2015 (https://edri.org/files/DP_BrokenBadly.pdf).

Report of the Nuffield Council on Bioethics (2015): "The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues", March 3, 2015 (http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf).

Rettberger, Jill W. (2014): Seeing Ourselves Through Technology How We Use Selfies, Blogs and Wearable Devices to See and Shape Ourselves, Hampshire: Palgrave Macmillan.

Rodriguez, Laura L./Brooks, Lisa D./Greenberg, Judith H./Green, Eric D. (2013): "The Complexities of Genomic Identifiability." In: Science 339/6117, pp. 275-276.

Rosenfeld, Michel (2002): "Hate Speech in Constitutional Jurisprudence: A Comparative Analysis." In: Cardozo Law Review 24, pp. 1523-1562.

Royal Statistical Society (2014): "The Data Manifesto", September 10, 2015 (http://www.statslife.org.uk/images/pdf/rss-data-manifesto-2014.pdf).

Sándor, Judit (2003): "Society and Genetic Information: Codes and Laws in the Genetic Era." Budapest: Central European University Press.

Schauer, Frederick (1982): Free Speech: A Philosophical Enquiry, Cambridge: Cambridge University Press.

Schwartz, Paul (1999): "Privacy and Democracy in Cyberspace." In: Vanderbilt Law Review 52, pp. 1609-1701.

Schwartz, Paul/Reidenberg, Joel (1996): Data Privacy Law: A Study of US Data Protection, Charlottsville: Lexis Law.

Spil, Ton/Klein, Rich (2014): "Personal Health Records Success: Why Google Health Failed and What Does that Mean for Microsoft HealthVault?" In: System Sciences (HICSS) 47, pp. 2818-2827.

Swan, Melanie (2012): "Health 2050: The Realization of Personalized Medicine through Crowdsourcing, the Quantified Self, and the Participatory Biocitizen." In: JMP 2/3, pp. 93-118.

Swan, Melanie (2013): "The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery." In: Big Data 1/2, pp. 85-99.

Tanne, Janice (2008): "Google launches free electronic health records service for patients." In: BMJ 336/7655, pp. 1207-1211.

Tene, Omer/Polonetsky, Jules (2012): "Privacy in the Age of Big Data: a Time for Big Decisions." In: Stanford Law Review Online 64, pp. 63-69.

University of Southern California's Annenberg Center for Digital Future and Bovitz.Inc Report (2015): "Surveying the Digital Future", December 10, 2014 (http://www.digitalcenter.org/wp-content/uploads/2013/06/2015-Digital-Future-Report.pdf).

Vodafone Institute for Society and Communications (2016): "Big Data: A European Survey on Opportunities and Risks of Data Analytics", January 3, 2016 (http://www.vodafone-institut.de/wp-content/uploads/2016/01/VodafoneInstitute-Survey-BigData-en.pdf).

Ward, Jonathan S./Barker, Adam (2013): "Undefined by Data: a Survey of Big Data Definitions." In: arXiv preprint arXiv: 1309.5821.

Warren, Samuel D./Brandeis, Louis D. (1890): "The Right to Privacy." In: Harvard Law Review 4/5, pp. 193-220.

Westin, Alan F. (1967): Privacy and Freedom, New York: Atheneum.

Wicks, Paul/Chiauzzi, Emil (2015): "Trust but Verify – Five Approaches to Ensure Safe Medical Apps." In: BMC Medicine 13, n. p.