amsterdamlawforum
VU University Amsterdam

SELLING MY SOUL TO THE DIGITAL WORLD?

Corien Prins[*]

"On Sunday, March 9, 2014, Googlezon unleashes EPIC". This quote is taken from a mini film-clip released in 2005 and written and produced by Robin Sloan and Matt Thompson of the Museum of Media History.[1] In their scenario, EPIC does not refer to the well-known public interest research centre in Washington, D.C. that was established in 1994 to protect privacy and constitutional values. Instead, in 2014, EPIC stands for the 'Evolving Personalized Information Construct'. In a fascinating story, Sloan and Thompson describe a future in which unparalleled search technology and detailed knowledge of individuals allow for total customisation of data and information. In less than ten years time, EPIC will stand for a "single source of content that contains everything that anyone could possibly ever want to know about."[2] Half of this period – five years – has passed. Where do we stand in the sketched scenario? Is it to become reality in another five years time? Do we indeed, silently and unconsciously, sell our souls to the unknown world of digital databases?

Indeed, in our information-intensive society, tailored and individualised services using numerous personal data appear to gain unprecedented popularity. New technologies such as mobile location-based services, Radio Frequency Identification (RFID), smartcards and biometrics support a greater capturing of customer and user information and allow services to be tailored to the individual's needs and desires. The prospects to private as well as public sector organisations are numerous: they range from the improvement of quality of service delivery and customer relations, to getting to know your customer, cost reduction, better achievement of organisational goals (e.g. profit, policy effectiveness), and effective enforcement of legal rights (e.g. copyright). Insight knowledge about individual customers, patients or citizens allows commercial and public sector organisations to address a large number of people on an individualised basis at the same time, not only within the territorial vicinity of the company or organisation, but even globally. It comes as no surprise that services designed on the basis of intelligent and personalised environments are the fastest growing segments of the digital economy, having spawned a multimillion-dollar industry.

---

[*] *Professor of law and informatisation at Tilburg University with the Institute for Law, Technology, and Society (TILT). Council member of the Dutch Scientific Council for Government Policy (WRR) in The Hague.*

[1] http://oak.psych.gatech.edu/~epic/

[2] For a transcript, see: http://www.masternewmedia.org/news/2004/11/29/summary_of_the_world_googlezon.htm

At the same time, we may observe that ICT-based highly personalised applications also offer individuals more and more opportunities to select how and with whom to interact, based on their own preferences. With mobile track and trace facilities, combined with web-based applications and different online channels it is becoming easier for individuals to find people, organisations, and/or communities with similar tastes and interests. People can now track and trace other individuals with similar preferences that are present within the same geographical space of about 30 metres. In short, personalisation seems to be an important, if not inevitable strategy to deploy numerous individual-centric activities and services.

A related and somewhat more recent development is what is often called 'ubiquitous computing'. Ubiquitous computing will create a context-aware environment in which numerous systems scan our environment for data and serve us with particular information, based on certain notions about what is appropriate for us as unique individual persons given the particulars of daily life and context. Some thus argue that ubiquitous systems will, to a large extent, structure and determine our daily life, mediating our identity, social relations and social power. Not only will our homes and working offices become public places, but our social identities as well. Anyone who takes a more in-depth look at these developments can see that the creation of EPIC as described by Sloan and Thompson, is indeed on its way.

Clearly, these developments trigger various concerns, for they may have profound effects on relationships between individuals, organisations and/or communities in our society. At the heart of these dilemmas is the very issue of user identification. It raises privacy problems as well as concerns with respect to inclusion and exclusion. Personalisation may be a threat to a user's privacy because it provides companies and organisations with a powerful instrument to know in detail what an individual wants, who he is, whether his conduct or behaviour shows certain symptoms, and so forth. Also, personalisation may be disturbing because it facilitates the selected provision to specific users only and may thus diminish certain preferences, differences and values. It is my belief that the debate on how to react to the emergence of the sketched developments, should therefore not be limited to a discussion on how to protect individual data. Instead, it should be a discussion about the impact on people's identity.

A key feature of personalisation is that individuals are given new ways to present and profile themselves – depending on the specifics of the context – in certain roles or 'identities'. They act as a certain type of citizen, consumer, patient, voter, etc. As a result, the growing importance of the context-specific concept of online identity raises challenging new questions with regards to the role and status of identity and identification. To what extent does the concept of 'online identity' get a different meaning compared to identity construction in offline relationships? Where exactly lie the boundaries between online identities and a person's 'own' or 'real' identity? In what

conditions may a certain fragmented or segmented aspect of a person's identity be considered an adequate representation of the 'real' person behind that identity? If online personalisation will become in part tantamount to the online identity of a person, then this state of affairs may raise the question of who may control the use of the data behind this identity as well as the identity itself? Can an online identity be owned? And if yes, in whom should such ownership be vested? Finally, new means of self-presentation also raises questions related to the reliability of identities and the implications of possible fraud with identities. To what extent can users 'play' with their online identity or virtual 'reputation', use their online reputation as a certain type of 'security', or even mislead organisations with a claimed online identity?

A more appropriate way to consider the implications of the sketched digital developments is by focusing less on the individual data, but instead, on the *effects* of the present-day technologies, in particular the almost limitless surveillance capacities of new technologies, such as location-based systems, radio frequency identifiers (RFIDs) and online personalisation instruments. In a sense, these surveillance techniques require that we shift our attention from individual sets of personal data toward the statistical models, profiles and algorithms with which individuals are assigned to a certain group or 'identity'. These models and algorithms are privately owned by businesses and corporations (trade secrets), and thus unavailable for public contestation. But the interests of personal data protection seem to require that they are made known to the public and thus are part of the public domain.

As previously mentioned, our behaviour in the 'public domain' is increasingly monitored, captured, stored, used and analysed to become privately-owned knowledge about people, their habits and social identity. Indeed, the term 'personal data protection' may lose its significance once we acknowledge this trend toward a commodification of identities and behaviour. It is this trend that is lacking in the present debate on personal data protection. Personal data are not used and processed anew and in isolation each time they are acquired by a company. In contemporary society, 'useful' information and knowledge goes beyond the individual exchange of a set of personal data. In 'giving' his or her personal data to a certain organisation, the individual does not provide these data for use in an 'objective' context. Today, the use and thus 'value' of personal data cannot be seen apart from the specifics of the context within which these data are used. Processing of personal data occurs within, and is often structured by, social, economic and institutional settings.

Thus, the question is not so much *whether* personal data are processed. They always are and will be, whether for legitimate or unlawful purposes. We create, implement and accept it ourselves by using the technologies that bring so much pleasure and comfort to our lives. Rather, we should direct our attention to *how* personal data are processed, in what context, and towards what end. Therefore, the focus of the discussion on privacy protection

should move away from the processing and use of single data. We need instruments to enhance the visibility of and knowledge of how personal data are used and combined, on the basis of what data individuals are typified, by whom and for what purposes. The debate should be redirected toward how individuals are typified (upon what social ontology, with what goal?) and who has the instruments and power to do so. In this sense, privacy is directly connected to position, social ordering, roles, individual status and freedom. Therefore, privacy protection in our present-day society should cover the capability to know and to control how our identities are constructed. It requires the availability of instruments to enable awareness of the context in which personal data are used and to monitor the data-impression that individuals are exhibiting to others. In other words, the discussion on the future of privacy protection must be a discussion on whether, and to what extent, the statistical models, profiles and algorithms that are used to generate knowledge about our individual behaviour, social and economic position, and personal interests, are transparent and controllable. Ultimately, it is precisely this discussion that is essential in the interest of societal values behind the concept of privacy, values such as autonomy, control, transparency and digital diversity.