Digital Alienation as the Foundation of Online Privacy Concerns

Brandt Dainow
Department of Computer Science, Maynooth University
Kildare, Co. Kildare
Ireland
+353 86 248 2846
brandt.dainow@nuim.ie

ABSTRACT

The term 'digital alienation' is used in critical IS research to refer to manifestations of alienation online. This paper explores the difficulties of using a traditional Marxist analysis to account for digital alienation. The problem is that the activity people undertake online does not look coerced or estranged from the creator's individuality, both of which are typically seen as necessary for the production of alienation. As a result of this apparent difficulty, much of the research has focused on the relationship between digital alienation and digital labour.

This paper attempts to overcome these difficulties by discarding the traditional approach. We argue one can better understand digital alienation by focusing on the relationship between user intent and technical infrastructure, rather than concerns with labour. Under the existing economic model dominating the internet, free services are financed by recording user activity and then using the products of this commercial surveillance to sell information about people to others. We show how the real harm in current online business models is that commercial surveillance is being used to commodify private life.

Seeking to define personal data in more precise terms, we will introduce two new concepts necessary for a detailed discussion of any ethical issues regarding personal data - the digital shadow and the digital persona. We will then show how affordances in current online systems are tuned to commodification of the user's personality. We will then explore the nature of online surveillance and show how affordances combine with the surveillance economy to produce digital alienation.

CATEGORY

[**K.4.1 Public Policy Issues**] – *Ethics, Privacy*

GENERAL TERMS

Management, Economics, Human Factors.

KEYWORDS

digital alienation, privacy, digital economy, surveillance, targeted advertising, personalization, critical theory, ICT ethics, Marxism

INTRODUCTION

Digital alienation is a privacy issue. Digital alienation occurs when one's digital lifeworld or the digital self is exploited. The process of exploitation extracts value from a person's digital activity through coercion and manipulation. We are coerced into submission to ubiquitous commercial surveillance[1] of our digital activity. Value is extracted from this surveillance process through the conversion of surveilled data into economic and political capital. The entire system represents a reification of one's digital lifeworld and commodification of the digital self. It also poses a number of problems for traditional understandings of concepts related to alienation within Marxist theory, such as coercion, exploitation, and power dynamics. Indeed, much of the debate in this area over the last few years has been concerned with how to account for alienation within a digital context. I believe the solutions to current problems can best be achieved by altering the analytic approach.

SCOPE OF CONCERN

Being connected to the ubiquitous computing environment which is coming to surround us is already necessary for full participation in modern Western societies. A review across the range of those emerging ICT's which will impact society over the next decade shows that being connected may become necessary for survival itself [35]. When the internet first emerged, it was predicted that it would "flatten" the power structures of traditional society, even lead to the "fading away" of the nation state [57]. Such views were based on technological determinism; they envisioned the new distinguishing features of internet technology as passing unmodified into society and reshaping it to match the internet's technical architecture [15].

In reality, the development of the internet ecosystem has been filtered through the structures of pre-existing society and evolved in accordance with its imperatives. While it has been disruptive in terms of changing some of the dominant players in media markets, destroying some and creating others, it has not fundamentally changed the power structures in society. Authoritarian governments have learned to control and censor it, hegemonic corporate capitalism has come to dominate it, and people's digital activities have been cajoled into closed silos controlled by a very few exceptionally large corporations [15]. Once seen as the antidote to structural inequality, the internet has actually become a profoundly powerful tool of domination based on exploitation and alienation.

ALIENATION IN CRITICAL IS STUDIES

The term 'digital alienation' is used in Critical IS research to refer to manifestations of alienation online. Stemming from digital labour studies [43] the focus soon bridged into social networking. A good example of this bridging can be seen in Fuchs and Sandoval's *Framework for Critically Theorising and Analysing Digital Labour* [25]. Initially exploring the dimensions of paid digital labour, the authors extend the analysis into the realm of

[1] Commercial surveillance involves the recording and analysis of online user behaviour with the aim of predicting and controlling their behaviour [81].

unpaid labour within content production in social networks. P.J. Rey's paper *Alienation, Exploitation and Social Media* [66] explores the mechanisms by which capitalism has come to exploit social media. Rey's task involves demonstrating how alienation exists within social networking as a dynamic of value extraction. This approach is also used by Christian Fuchs [23,25] in most of his work. By contrast, Krüger and Johanssen's *Alienation and Digital Labour—A Depth-Hermeneutic Inquiry* [43] examines alienation through a survey of prosumer's comments about social network's themselves. Here alienation is demonstrated through the effects of the social network system's activities, rather than through the dynamics of labour and surplus value extraction. If alienation can derive from unpaid digital labour, as seen in social networks, the possibility arises that alienation can be found wherever unpaid digital labour occurs. Here we find Marc Andrejevic's *Surveillance and Alienation in the Online Economy* [6], which extends the analysis of alienation beyond social networking into general online activity. This paper shows a third approach to explaining digital alienation by focusing on exploitation, in contrast to the previously mentioned papers, which focus on value extraction and coercion. What all these analyses demonstrate is that the nature of alienation online necessarily diverges from the account of alienation in earlier, pre-digital, analyses. These divergences reflect the differences in structures of production and value-extraction between analogue and digital socio-technical systems. These differences are significant to the degree we may warrantably talk of a distinct "digital" form of alienation.

In Marx, alienation is the result of labour activity coerced into alienated forms in order to produce products estranged from the producer [60]. The political dynamic is the extraction of value from controlled and structured worker activity. Historically, analysis of digital alienation has focused on accounting for the traditional mechanisms underpinning alienation within a digital context. There has been an unspoken consensus that an account of digital alienation requires identifying the same structures and mechanisms within the digital context as Marx identified within the factory. Here the concern is to understand digital alienation by analysing it as the result of conditions considered necessary for alienation - coercion, labour and estrangement from product. With regard to coercion, the difficulty is whether people who freely choose to use social networks like Facebook can be described as coerced. The concern with labour is whether people's unpaid production of content in social networks can be described as labour. Finally, if people seem to be expressing themselves within social networks, the question arises as to how can they estranged from the output of their activity.

At one extreme researchers such as P.J. Rey have argued that the differences between the Victorian factory of Marx's analysis and modern digital activity are so great that alienation is a questionable concept within a digital context [66]. Rey argues that the products of digital labour in social networks are not alienated because creation of this content is freely chosen and creative. Referring back to Marx's categorisation of imagination as a distinguishing characteristic between animals and humans, Rey suggests that the creative nature of social content production renders the output unalienated. His view is that the creativity involved in social network content creation allows the producer to recognise themselves within their output. In addition, the free choice to engage in social networking means this labour is uncoerced. Rey does accept there is some degree of exploitation involved because social networks derive financial value from this output without financially compensating those who produced it. However, he argues this exploitation is mild because producers do receive compensation in other forms of capital. Rey argues that social network users are compensated because they retain use of their output for their own purposes. They can therefore use the content they produce to generate social and cultural capital. His position is that the non-economic value derived is so great that any exploitation is "relatively minimal" [66:415]. Furthermore, any exploitation present is, Rey argues, further diminished by the unalienated nature of prosumer output. Rey acknowledges that social networks also derive value from surveillance of user activity, usually without users being aware of it. However, while he sees this as mildly exploitative, he does not consider it alienating. Rey's position is that digital capitalism can maintain the inequalities and power structures within society identified by Marx, but without the need for alienation, or even very much exploitation.

It is notable that, while recognising that social networks extract value from user surveillance, Rey does not extend this recognition to the fact, noted by others, that such surveillance is almost universal throughout the internet [51,81]. A 2012 study of the world's busiest websites revealed that 94% engaged in some form of user surveillance themselves, half of whom also allowed unidentified third parties to engage in such tracking through their sites. The same study also found that 91% of these sites changed their content to match their understanding of the user [70], something impossible without a pre-existing knowledge of that user; knowledge which can only have come from previous surveillance. User activity in other parts of the internet, such as search and reading, does not generate cultural or social capital, but is still subject to the same levels of commercial surveillance. Following the logic of Rey's analysis, this renders such surveillance much more exploitative. In general, Rey's analysis treats technology as invisible and as permitting users to fully express themselves in an unmediated fashion. While Rey recognises that surveillance occurs, he fails to take into account that much it is used to tune and filter the online environment surrounding the user. Users are presented with "personalised" choices, links and content based on the results of covert surveillance as much as on the content they produce; something often referred to as the "filter bubble" [56,65]. People are therefore not able to make free choices or even fully express themselves, because the technology available to them is not value-neutral, but tuned to commodification [19,39].

Andrejevic's analysis of digital alienation is founded on just this consideration. All internet users are subject to pervasive universal surveillance by commercial enterprises [16,70,79,81]. The value of this surveillance far exceeds that derived from social network content creation [16,20,29,51,79,81]. Initially this information was used only to tune advertising delivery [16,81]. However, this information is now also used to tune the delivery of news on many sites [81] and for political manipulation [1]. Users have no choice over whether their activity online is recorded, processed and used, nor do they know who by [70]. This constitutes, for Andrejevic, alienation. His argument is that the lack of choice over whether to be surveilled or not constitutes a structurally-embedded coercion. He further argues that the lack of knowledge about this surveillance constitutes an epistemological alienation. Finally, he argues that the use of this information to alter content in an effort to manipulate the user fits Marx's definition of alienation as an estranged power structure working against the individual [6,8].

In contrast to Rey's position that exploitation is mild because the user derives non-economic use-value from the content they create, Christian Fuchs [23] has argued that exploitation is either present or not, and cannot be present in variable degrees. One cannot be a little bit exploited. Fuch's work tends to focus on the mechanisms of value-extraction within a digital context. Fuch's position is that any activity conducted by someone which can be used to generate economic value is labour. He seeks to bring together the competing positions held by Andrejevic and Rey by arguing that Rey is focused on subjective feelings of alienation whereas Andrejevic is focused on the objective conditions of non-

control and non-ownership. However, Fuchs firmly comes down on the side of alienation being objectively present, arguing that the purported social use-value that content creators derive from their work hides the true commodity character of social networking [24]. He identifies two dimensions of value within social networks - the value of created content and the value of user presence. Here Fuchs agrees with Andrejevic that the users of social networks are themselves treated as commodified products which are then sold.

Both Fuchs and Andrejevic limit their conception of the use of personal data to the realm of advertising delivery. While the first use of this information was indeed to tune content, especially advertisements, to the user profile, this information is now also sold for other purposes, including political manipulation [1], credit scoring [54,72], housing and employment [12] and news delivery [81]. It is worth noting that both Facebook and the international trade body for online advertising, the Internet Advertising Bureau, agree with this assessment of where the real value lies in commercial online surveillance [16,20]. In comparison with this vast and pervasive surveillance industry, user-generated content within social networks is a trivial consideration. Under this analysis, alienation is a pervasive and unavoidable adjunct to almost all digital activity.

Rey, Andrejevic and Fuchs all approach alienation within a digital environment by focusing on Marx's mechanisms for its production and explaining how and where these mechanisms can be found online. While general commercial surveillance is mentioned, it is not really the central focus of their analysis, nor does it alter their approach. My position is that we can better account for digital alienation if we can liberate ourselves from the form of Marx's account. Marx provided an analysis of how alienation occurred within a particular historical and technological context. As we have seen from the above, we encounter problems if we assume that this is the only mechanism by which alienation can occur or that all of these traditional mechanisms are necessary. My argument is that the features of digital alienation are so different from traditional alienation that a new account is necessary.

HOW ALIENATION OCCURS ONLINE

In defining alienation, Marx considered two factors, the nature of alienation and the means by which it is produced. The nature of alienation is that the individual is disconnected from the products of their labour by property ownership rights; they are alienated from ownership of both the product and the means of producing it. This constitutes the material base of alienation and is the product of power relations governing the production process. Marx's account involved material coercion by controlling access to the means of survival so as to force people into alienating labour. Analysis of exploitation on the internet has been distracted by the apparent lack of coercion motivating online activity and by the appearance of self-expression in social networks. However, our analysis becomes less complicated if treat social networking within the broader context of pervasive digital surveillance. Here we recognise that, while content production in social networks is voluntary and can be self-expressive, it is just one type of action within the wider class of voluntary and self-serving digital activity which includes search, shopping, email, use of maps, health trackers, life loggers and other digital services, not to mention general web surfing. This is important because the range of digital activities will continue to spread until it permeates most of our environment [63]. Because of this it is essential to treat the current state of affairs as an intermediate process moving towards more ubiquitous computing. Our analysis must recognise that the political and economic structures which affect us within the current digital domain are on a trajectory to dominate our entire existence, offline as well as online. It is important, therefore, to recognise that the frame of analysis cannot limit itself to voluntary activity knowingly making use of digital services. The infrastructure being created now will one day support smart cities, the internet of things, and digital devices implanted within our bodies. Our entire existence will become mediated through digital services within a few decades [63].

Thus the place of labour as seen in a traditional account of alienation becomes problematic when value is being extracted from broad-spectrum use of digital services for life in general. Assuming that labour is a necessary precondition for alienation requires explaining how all activity using digital services constitutes labour despite the fact it generates no obvious income and may not even be anything more than a traditional activity, like walking or driving, which has been supplemented with a digital component. Certainly the argument of remuneration in the form of social or cultural capital is inapplicable with reference to activities which do not involve any form of communication, such as using search engines or passively reading a website, yet value is extracted from these activities by others via commercial surveillance [8,11,16,62,69,73,81]. If we redefine 'labour' as referring to any activity from which value may be drawn by any party, as Fuchs does [23,24], then almost all activity becomes labour and the term ceases to provide any real distinction from other mode of activity. I think it is better to abandon the issue of whether online activity is labour or not. There is nothing within Marx's description of alienation which requires that it must, of necessity, derive from labour. 'Alienation' in Marx is not a single concept, but a translation of two terms, *Entfremdung* and *Entäusserung*, which can also be translated as 'estrangement' and 'externalization' respectively [60]. These terms are applied to a variety of phenomena, including internal mental states, property relations and societal structures. It is true that Marx attempts to provide a systematic analysis of political economy based on the concept of alienated labour in his early work, but that attempt is incomplete [86]. In his later works, alienation becomes a descriptive term which is applied to multiple phenomena. There is nothing in his usage which locks alienation to labour except as a historically contingent feature of nineteenth century capitalism [86]. All that is required by Marx's account is that there be human activity and that this occur within certain types of unequal power structure within the field of economic competition.

On this basis, I propose to focus on digital alienation as a product of property relations regarding data. Surveillance is a process of data acquisition; some generated as the output of online surveillance monitoring systems and some data taken from elsewhere, such as the passenger name records used for international travel, geo-location data and credit scores [1]. The common element all these data elements have is that they are held to pertain to the same individual[2]. The dataset created is termed a "personal profile", as opposed to group profiles [31,38]. The personal profile is a digital representation of an individual. It is the central commodity of the surveillance economy. Each organisation which holds a personal profile subjects it to algorithmic analysis and manipulation in order to extract value from it. The term used in the industry is to "monetize" it. It is this profile which is used to tune content and for purposes of manipulation. All actions using personal data draw that data from the personal profile. Such use constitutes Marx's concept of an environment which reflects back on the producer estranged output [8]. In that surveillance technology produces the personal profile as a commodity, it is a type of production process. The raw material for this production process is the activity of individuals [32], which is used to produce personal profiles. This production process is not owned by those who generate the activity which

[2] This belief may be mistaken, it is not always possible to distinguish between a person and a device; and cases of mistaken identity also occur.

feeds it. This is the basis for alienation from ownership of the means of production. The surveillance process is hidden and unwelcome [14,32] and therefore represents an unequal, coercive and exploitative power structure [8]. We may view the personal profile as a field of contention between commercial surveillance companies and those who use their products on one hand opposed by individuals and privacy advocates on the other.

The essential starting point to all forms of alienation is individual activity. I therefore believe we may best understand digital alienation by examining the mechanisms by which an individual's digital activity is alienated. Here we must focus on the nature of personal action within a digital context, the mechanisms by which the personal profile is generated, and the use to which it is put. As mentioned above, the first task is to dispense with the need for a concept of labour. In Marx's analysis labour was the term used to distinguish activity which supported alienation from activity which did not. Labour supported alienation because it was activity which occurred within, and was shaped by, exploitative power structures. However, no such distinction between labour and non-labour exists online because all activity is surveilled and exploited [73,81]. Not only does discarding the need for labour ease our analysis, I believe it helps to direct our attention to the ubiquity of digital surveillance. Instead I will define human activity within a digital context in terms of people's intentions and expectations. To do this I will introduce distinguish the two targets of surveillance; communicative activity and everything else. I will refer to these as the 'digital persona' and the 'data shadow', respectively.

'Digital persona' is the term I propose for the body of digital material created by an individual through acts of online communication. The digital persona includes blogs, comments, product reviews, tweets and other social network postings, together with any other conscious communication by an individual within a digital context. Thus the digital persona is created by the individual to express and communicate. The digital persona is not a direct or unmediated reflection of the personality, but a creation through which the individual seeks to represent of an aspect of themselves. The disconnect between the offline and digital world permits people to exaggerate or repress particular aspects of their personality [77]. For example, introverts may use the digital persona to compensate for difficulties they have in face-to-face interactions [3] while extroverts often use it to confirm pre-existing characteristics [82]. In other cases, people develop new personal characteristics online so that they can incorporate them into their offline personality [53]. In all cases, what is revealed or portrayed is further influenced by previous experiences online, especially concerns over privacy and security [42,87]. I derive the term 'persona' from C. G. Jung's concept of the persona as a creation of the ego designed to represent a subset of that ego within specific social circumstances [36]. The same idea is used within a sociological perspective in Goffman's *The Presentation of Self in Everyday Life* under the term 'masks' [28], which outlines his Dramaturgical Theory, a sub-set of Symbolic Interactionism [68].

The term 'data shadow' was first used by Alan Westin in *Privacy and Freedom* [84], but has entered into general use both in computing and privacy discussions. It refers to the information generated by someone as a side-effect of their use of digital technology. These days this includes log files, access records, search histories, movements between and within web sites, mobile phone location records and all financial activities not involving cash [11,31,39]. Thus the term 'data shadow' refers to all digital information pertaining to an individual which they did not consciously and intentionally create for communicative purposes. This information may have been generated by the user for other purposes, such as their "click-stream history," which is a record of their mouse click activity within a website [32], or their "search history," a record of all the searches they have made in a given search engine. Elements of the data shadow can also be generated through the monitoring and recording of user activity by other systems. For example, web server log files, containing records of every file request, constitute data generated by the system about the user. The term 'data shadow' includes the material used to commodify users within social networks, but also applies outside social networking. Data shadows may be created through any and all use of digital technology.

Data shadows are created by a network of commercial surveillance agencies whose tracking technologies permeate digital services [11,16,46,51,81]. Very few of these agencies are known to the public [11,73]. Some, like Google and Facebook, are well known because of their public profile as digital service providers, though their activity as commercial surveillance agents is less well known, even though it drives their profits [20,29]. Others, such as DoubleClick, Acxiom, Experian and BlueKai are known to industry analysts and privacy advocates as a result of their scale and reach. However, the majority, such as ClickTale, Optimzly, Kiss Metrics, Info Group, Ace Metrics, Crazy Egg, Site Meter, Moz, Adgistics, People Metrics, Data Dog, Data Mentors, Extrawatch, Inspectlet, eDataSource, Prognoz, and literally hundreds of others, are unknown outside the specialist profiling industry. No one knows how many of these agencies there are, or what they do, but it is known they combine the data they gather with information from other sources to create detailed profiles on literally hundreds of millions, if not billions, of people [11,21,83]. The commercial surveillance industry is much larger in terms of economic value and user-base than any other online industry [16,73,81].

This universal commercial surveillance means there is no way to use most digital services without being surveilled [21,32,73,81,83]. For most digital services there is no alternative provider who does not practice surveillance (or permit others to do so) within the service stream [76,81]. However, lack of choice most strongly stems from lack of knowledge. We are simply unaware of when we are being surveilled, who by and for what purpose [32,79]. Obviously, one cannot exercise choice over things one is unaware of. As we have seen, this lack of choice has been held to constitute coercion by Andrejevic and Fuchs, but not by Rey. Lack of choice as coercion has a long history of support in philosophy. For example, Aquinas argues that coercion occurs when actions by one person mean someone cannot act otherwise [10]. However, this position was challenged in the twentieth century by the position that coercion requires communication between the coercer and their target, usually in the form of conditional threats [2]. Under this view coercion is a communicative act, not a contextualising situation. This is the position currently supported in much legal practice, especially in the USA [5]. However, since the 1980's arguments have re-emerged in support of structural coercion; the creation of situations in which one is prevented from selecting alternative courses of action [67]. Here the focus is shifted to the coercer's intentions to remove choice from another [4]. This accords with much of Marx's analysis in which he focuses on the general circumstances of capitalist society as coercive in the sense of removing freedom [86]. Clearly, hiding surveillance so that people cannot avoid it constitutes removal of choice and diminution of freedom. Thus it is possible to argue from this perspective that the lack of choice to avoid surveillance constitutes coercion. However, we must recognise that this position is not in accord with how many, especially in jurisprudence, understand the term.

Lack of choice, even coercion, does not automatically mean that the output of a productive process is alienated. I wish therefore to explore the mechanism by which digital activity becomes alienated. Since we have two forms of digital data, the digital

persona and the data shadow, two accounts are necessary. I shall commence with the alienation of the digital persona.

EGO, AFFORDANCES AND THE DIGITAL PERSONA

People use Web 2.0 technologies to create their digital persona. The process by which they do this, and the persona they create, are alienated. We therefore need an account of the mechanism by which people do this and how alienation occurs. Central to my account of how the digital persona is alienated is the view of technology as a socio-technical system [35]. A technology may be composed of multiple artefacts and may be "read" or understood in different ways [30,34]. The nature of the "reading" depends on the person, their social environment, past experiences and other factors, all of which are constrained by the functional capabilities of the artefacts in question [58]. We therefore need a conceptual framework which holds all the dynamics which are at play in a person's understanding and use of a technical system. I will use the concept of "affordances" to explain the interaction between people and the technical artefacts.

The concept of affordances originates with James Gibson's conceptualisation on the subject of how animals perceive and understand their environment in *The Ecological Approach to Visual Perception* [27]

> "The affordances of the environment are what it offers the animal, what it provides or furnishes, either for good or ill… It implies the complementarity of the animal and the environment… [affordances] have to be measured relative to the animal. They are unique for that animal. They are not just abstract physical properties." [27:127]

Gibson was arguing against a reductionist understanding of perception and for a perceptive process within all animals in which perception itself is not merely a process of physical activity onto which understanding is overlaid *post hoc*. Instead, he argued that the perceptive process itself incorporates cognitive elements such as motivation, environmental context and past experience into the act of seeing.

The concept was applied to ICT analysis by Ian Hutchby in *Technologies, Texts and Affordances* [34], in which he describes technologies as

> "Texts which are written in certain ways by their developers, producers and marketers, and have to be read by their users or consumers. The writers of these technology texts may seek to impose particular meanings on the artefact, and to constrain the range of possible interpretations open to users. Users, by contrast, may seek to produce readings of the technology texts which best suit the purposes they have in mind for the artefact… Neither the writing or reading of technology texts is determinate: both are open, negotiated processes. Although there may be ways that technology texts have preferred readings built into them, it is always open to the user to find a way around this attempt at interpretive closure." [34:445]

We may thus see affordances as a field of competition in which the owners of a technology compete with the users of that technology for domination of the affordances dictating how that technology is understood and used. Donald Norman explores this competition over technological affordances in *The Design of Everyday Things* [58]. In Norman's account, we use affordances to build conceptual models of how things work. Any technology involves the interaction of two conceptual models; a design model and a user model. The design model is the conceptual model held by the designers when they built the technology and in accord with which they try to construct the artefact. The user's model is the conceptual model users have of that same technology. Norman is concerned with what happens when the two models clash or diverge. According to Norman, there is no necessary convergence between the user's mental model and the designer's. In fact, in Norman's view, the two model's clash most of the time. Using Norman's framework, I suggest that the user model conceptualises the Web 2.0 services people use to express their digital personas as private, unmediated and natural. The user model fails to recognise the degree of surveillance and the degree to which their activities are mediated through a technology designed for data gathering and commodification. Users also fail to recognise the degree to which surveillance is used to filter and control the content they see in social networking and news sites and in advertising. Instead, users see the content presented to them within social networks as somehow neutral, unmediated and unsurveilled [71]. In contrast, service providers, such as Google and Facebook, show evidence of believing that users have the same conceptual model as designers. They have countered concerns over online privacy by stating users have no expectation of privacy and accept that the material they create will be processed for purposes of commodification [22].

There are numerous studies which demonstrate that users manipulate their self-expression online in order to convey specific characteristics and control the image others have of them [41,50,53,82]. In our terminology we may say people use Web 2.0 technologies to construct their digital personas. Their understanding of what can be expressed, the values determining what should be expressed and how this is to be done are determined by the affordances users perceive in these technologies [74,89]. These affordances constitute what Groffman describes as the "props and tasks" [28:143] which dictate what persona[3] is appropriate and the "expressive resources" [55:74] available from which to construct it.

Unfortunately for users, Facebook and similar Web 2.0 systems are not designed for people to portray themselves in any manner they may choose. Instead, Facebook and similar systems divide personal characteristics into a set of discrete data points, such as preferred objects of consumption, marketable skills, and approvable attitudes [33]. Furthermore, qualitative characteristics, such as friendship, are reduced to quantitative values, such as the number of likes or followers. Facebook's affordances, in particular, suggest to users that their digital persona is a true reflection of their identity, yet is at the same time something to be constructed, managed and enhanced [26]. Facebook openly expresses the neo-liberal concept of a "personal brand," in which a person creates a commodified public image as the repository of their social capital [44]. The affordances of Facebook present the individual as composed of consumption patterns (such as preferred movies, books and music) and patterns of association (as shown through one's likes, friends and photos). These are dimensions of analysis more suited to processing for advertising than developing an understanding of the whole person. There is good empirical evidence that this model conflicts with the affordances the user brings to Facebook. In many cases users seek to express themselves in ways restricted by the affordances Facebook imposes, resulting in dissatisfaction, resistance and disuse [26,42,50,74].

In using affordances tuned to atomising, quantifying and commodifying the depiction of people, social media systems like Facebook alienate the digital persona. Rather than a free expression of the self, users are forced to display only those characteristics which are commodifiable. These characteristics are then embedded in a manipulated content environment which reinforces and promotes ongoing commodification, and therefore

[3] Groffman's term is "performance" [28:143]

embeds the alienated digital persona within an alienated social environment.

ALIENATION AND THE DATA SHADOW

The mechanisms by which the data shadow is alienated are straightforward compared to the digital persona and commence with unavoidable, hidden, ubiquitous commercial surveillance [70,73,81]. In that the digital world is permeated with unknown entities gathering unknown information to use for unknown purposes [21,83], the digital environment is self-evidently epistemologically alienated from the user. The material base of the commercial surveillance system supports a superstructure devoted to exerting power over the individual by influencing their behaviour directly, or by influencing decisions made about them by other people [11,72,80]. This is achieved through personalization of content [56], such as the advertising [78] and news [81] to which people are exposed.

The unavoidability of commercial surveillance is made possible by the lack of ownership or control users have over digital services. It is known that, in general, people do not like commercial surveillance or content personalization [14,17]. Commercial surveillance therefore constitutes the exercise of power over individuals and a diminution of their freedom, another manifestation of alienation [7]. Furthermore, the knowledge that unknown surveillance is occurring, in combination with lack of knowledge about how that information is used, has a chilling effect on people's online activities [32,49,75]. In effect, people are alienated from their own actions online before they perform them. In that this chilling effect also applies to how people communicate online, ubiquitous commercial surveillance further alienates people from each other.

DIGITAL ALIENATION – THE COMPLETE PICTURE

We are now in a position to provide an account of how the four dimensions of alienation occur. First, users are alienated from their productive activity through restricted affordances within expressive Web 2.0 technologies which promote a commodity fetishism of personal characteristics and interpersonal relationships. This is made possible by an alienated power structure which is designed around treating users as commodities [8,23]. Users are alienated from non-expressive activity by the presence of ubiquitous hidden surveillance systems. Thus users are alienated from all forms of digital activity. Second, users are alienated from the products of their digital activity by property relations. These grant service owners the right to reuse user-produced content for their own purposes and to process both the digital persona and the data shadow in order to construct personal profiles. Users are further alienated from the products of their own activity since the personal profile is used against them, either to manipulate their behaviour or to influence how others treat them. In addition, the abandonment of the open standards which created the web means that the products of user activity are imprisoned within data silos owned by service providers [18]. Thus, you may close your Facebook account, but you can't move it to another social network. Third, users are alienated from each other by the necessary mediation of fetishizing social networks and by the chilling effect of ubiquitous surveillance. Finally, users are alienated from themselves and their own human potential in three ways; through the imposition of fetishizing affordances promoting the concept of the personal brand, through their limited control over their own digital persona, and through the use of personalization technologies which confine the user's ability to discover the unexpected, the unusual, and the uncommodified.

SOLUTIONS

No solution exists today which can resist these patterns and structures of digital alienation. However, a number of technologies exist which can form part of a solution, while the design principles to complete the solution are understood. Two related characteristics support the existence of digital alienation, lack of choice and lack of power. The solution is therefore to restore choice and empower the user. In my view solutions that look to regulation, such as data protection and privacy laws, merely perpetuate a hierarchical structure which keeps people in a powerless position. Instead of companies deciding what to surveil, we merely pass the decision to legislators. Given the history of government digital surveillance [9] there is nothing to suggest this improves matters. In addition, the impossibility of a single legislative framework for the entire internet [64,85,88] means surveillance companies can simply move to more conducive regimes. Furthermore, centralised storage of personal data is frequently subject to leaks [40,47,48], so I am opposed to centralised storage of any fashion, never mind under what rules.

The first task in combating alienation must be to remove coercion from the situation by giving users the choice over whether to be surveilled and for what purpose. A number of technologies exist which can offer elements of this solution. Anonymizing systems such as such as TOR [52] and TextSecure [61] enable users to avoid being tracked while using the existing internet. These need to be extended and built into a comprehensive set of easy-to-use systems which can wrap browsers and other applications in a protective and intelligent layer which negotiates and controls what data is accessed by what services. Protocols like the W3C's Platform for Privacy Preferences (PPP) [13] can form the basis for such communications. Design of data gathering systems should follow principles of privacy preservation, such as those developed by Marc Langheinrich [45], one of the authors of PPP. Such technology would enable users to control how much information is gathered about them and thus how much personalization is possible. This de-alienates the productive technology by putting control in the hands of the user and de-alienates their digital environment by permitting them to control or prevent personalization.

While these solutions restore choice to the user, they only partially redress the balance in an existing system which is structurally inequitable. The long-term solution must therefore be to move personal data storage, and therefore ownership, into the hands of the users. Here the solution is to reverse the cloud architecture. Currently, centralised systems run analyses of locally held data. I propose inverting this structure, such that personal data is held by the person in their own devices. Effectively each person, or home, would operate their own data store. Following Langheinrich's privacy-preserving design principles [45], devices would, wherever feasible, store their own data. A personal server or gateway would provide the interface between digital service providers and the user's personal data. This gateway would be able to negotiate access for services and prepare personal data for access. This pre-processing would anonymise the data to the degree selected by the user for that type of service. I envision this system working in a manner similar to hierarchical protection domains (or "security rings") within chipsets. These create a series of layers within which particular software operations can be confined so as to shield the system from inappropriate operations [37]. Corporate digital services could still be centrally managed and owned, but their computations would have to call on the individual's own data store rather than house it on corporate servers.

This is, however, merely a collection of artefacts. As a socially-embedded system, technology needs more than just hardware if it is to be adopted. The additional component required is therefore societal structures promoting and maintaining such a system. A

network of local technicians is required to maintain and develop such systems, provide advice and training, lobby regulators for support and so forth. Here I suggest the basis lies in recognising the value of personal data. For example, the value of a Facebook user is between $US40 and $US300 [59]. If personal data has value for service providers, let them pay for it. A system of micropayments for access to personal data would create a data economy enabling individuals to earn money through the gathering and storing of their own data. Support agencies, such as technical staff and software vendors, can then be remunerated through a share of this income. Such a system would permit the development of an intermediate layer of data vendors who can store and provide personal data on the user's behalf, according to guidelines provided by those users, or remotely maintain data held in the home. Such a system permits of multiple organisational models. Community groups could operate such services. For example, people who share the same set of data access protocols could form cooperatives to manage storage and access to their member's data. As yet, such technology does not exist. However, the hardware is already in place. Personal cloud storage devices have been available for several years. These permit users to store their data in their home while still being able to access it remotely. The missing components are therefore the micropayment and data negotiation systems. Protocols exist which can handle both, they merely need to be implemented as working products.

We need to bear in mind that the digital service infrastructure we see today is merely a step towards a digital environment of ubiquitous devices; embedded within our bodies, throughout our homes, offices, cars and public spaces. A critical evaluation of current data practices must consider this long-term future and seek emancipatory paths within it. As we have seen, digital alienation is the product primarily of inequitable power structures which intentionally deny users control, or even knowledge, of what is being done to them. The motive power of these structures is the economic value of personal data. If digital services are to align with individual needs, we cannot avoid personal data being processed. The solution is therefore to develop systems which pass some of that value back to the user. Doing so gives the user power and makes them a viable partner for other organisations who can earn a living by controlling access to personal data on behalf of the user. Giving the individual control over their personal data emancipates them from subjection to hegemonic digital capitalism by permitting them to negotiate the terms of the relationship they have with their digital service providers.

REFERENCES

[1] Nathan Abse. 2012. *Microtargeted Political Advertising in Election 2012*. Internet Advertising Bureau, New York, NY, USA. Retrieved from http://www.iab.net/media/file/Innovations_In_Web_Marketing_and_Advertising_delivery.pdf

[2] Timo Airaksinen. 1988. An Analysis of Coercion. *Journal of Peace Research* 25, 3, pp. 213–227.

[3] Yair Amichai-Hamburger, Galit Wainapel, and Shaul Fox. 2002. "On the Internet No One Knows I'm an Introvert": Extroversion, Neuroticism, and Internet Interaction. *CyberPsychology & Behavior* 5, 2, 125–128. http://doi.org/10.1089/109493102753770507

[4] Scott Anderson. 2008. Of Theories of Coercion, Two Axes, and the Importance of the Coercer. *Journal of Moral Philosophy* 5, 3, 394–422. http://doi.org/10.1163/174552408X369736

[5] Scott Anderson. 2010. The Enforcement Approach to Coercion. *Journal of Ethics and Social Philosophy* 5, 1.

[6] Mark B. Andrejevic. 2011. Surveillance and Alienation in the Online Economy. *Surveillance & Society* 8, 3, 278–287.

[7] Mark B. Andrejevic. 2011. Estrangement 2.0. *World Picture* 6, 1–14.

[8] Mark B. Andrejevic. 2012. Exploitation in the Data Mine. In *Internet and Surveillance*, Christian Fuchs, Marisol Sandoval, Boersma Kees and Anders Albrechtslund (eds.). Routledge, New York, N.Y, 71–88.

[9] Julia Angwin. 2014. Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance. Henry Holt & Co, New York, N.Y.

[10] Thomas Aquinas. 1920. *Summa Theologica*. Fathers of the English Dominican Province, London.

[11] Nathan Brooks. 2005. *Data Brokers: Background and Industry Overview*. Congressional Research Service, The Library of Congress, Washington, D.C.

[12] Danielle Keats Citron and Frank Pasquale. 2014. The Scored Society. *Washington Law Review* 89, 1, 1–33.

[13] Lorrie Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, and Joseph Reagle. 2002. *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*. W3C. Retrieved from http://www.w3.org/TR/P3P/

[14] Mary J. Culnan. 1993. "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS Quarterly* 17, 3, pp. 341–363.

[15] James Curran, Natalie Fenton, and Des Freedman. 2012. *Misunderstanding the Internet*. Routledge, London.

[16] John Deighton and Lenora Kornfield. 2012. *Economic Value of an Advertising-supported Internet Ecosystem*. Internet Advertising Bureau, New York, N.Y. Retrieved from http://www.iab.net/insights_research/industry_data_and_landscape/economicvalue

[17] Jenny van Doorn and JannyC. Hoekstra. 2013. Customization of Online Advertising: The Role of Intrusiveness. *Marketing Letters* 24, 4, 339–351. http://doi.org/10.1007/s11002-012-9222-1

[18] Tony Dyhouse. 2010. Addressing the Silo Mentality. *Infosecurity* 7, 2, 43. http://doi.org/10.1016/S1754-4548(10)70043-7

[19] Fredrik Erlandsson, Martin Boldt, and Henric Johnson. 2012. Privacy Threats Related to User Profiling in Online Social Networks. *Proceedings of 2012 International Conference on Social Computing*, IEEE, 838–842.

[20] Facebook Inc. 2014. *Facebook Inc. First Quarter 2014 Results*. Facebook Inc. Retrieved from http://investor.fb.com/releasedetail.cfm?ReleaseID=842071

[21] Federal Trade Commission. 2014. *Data Brokers: A Call for Transparency*. Federal Trade Commission.

[22] Jeremy Fogel. 2014. A Reasonable Expectation of Privacy. *Litigation* 40, 4. Retrieved December 15, 2014 from http://www.americanbar.org/publications/litigation_journal/2013-14/spring/a_reasonable_expectation_privacy.html

[23] Christian Fuchs. 2013. Class and Exploitation on the Internet. In *Digital labor - the Internet as playground and factory*, Trebor Scholz (ed.). Routledge, New York, 211–224.

[24] Christian Fuchs. 2014. *Digital Labour and Karl Marx*. Routledge, Taylor & Francis Group, New York, NY.

[25] Christian Fuchs and Marisol Sandoval. 2014. Digital Workers of the World Unite! A Framework for Critically Theorising and Analysing Digital Labour. *tripleC* 12, 2, 486–563.

[26] Ilana Gershon. 2011. Un-Friend My Heart: Facebook, Promiscuity, and Heartbreak in a Neoliberal Age. *Anthropological Quarterly* 84, 4, 865–894.

[27] James Jerome Gibson. 1986. *The Ecological Approach to Visual Perception*. Psychology Press, New York.

[28] Erving Goffman. 1990. *The Presentation of Self in Everyday Life*. Doubleday, New York, NY.

[29] Google Inc. 2014. *Google Inc. First Quarter 2014 Results*. Google Inc. Retrieved from http://investor.google.com/earnings/2014/Q1_google_earnings.html

[30] Martin Heidegger. 1977. The Question Concerning Technology, and Other Essays. Harper & Row, New York.

[31] M Hildebrandt. 2008. Defining Profiling: A New Type of Knowledge? In *Profiling the European Citizen*, M Hildebrandt and Serge Gurtwith (eds.). Springer, New York, NY.

[32] Simone van der Hof and Corien Prins. 2008. Personalisation and its Influence on Identities, Behaviour and Social Values. In *Profiling the European Citizen*, M Hildebrandt and Serge Gurtwith (eds.). Springer, New York, N.Y, 111–127.

[33] Gordon Hull, Heather Richter Lipford, and Celine Latulipe. 2011. Contextual Gaps: Privacy Issues on Facebook. *Ethics and Information Technology* 13, 4, 289–302. http://doi.org/10.1007/s10676-010-9224-8

[34] Ian Hutchby. 2001. Technologies, Texts and Affordances. *Sociology* 35, 2, 441–456. http://doi.org/10.1177/S0038038501000219

[35] Veikko Ikonen, Minni Kanerva, Panu Kouri, Bernd Stahl, and Kutoma Wakunuma. 2010. *D.1.2. Emerging Technologies Report*. ETICA Project.

[36] C. G. Jung. 1977. The Collected Works of C. G. Jung. 6: Psychological types. Pantheon Books, New York, NY.

[37] Paul A. Karger and Andrew J. Herbert. 1984. An Augmented Capability Architecture to Support Lattice Security and Traceability of Access. IEEE, 2–2. http://doi.org/10.1109/SP.1984.10001

[38] Helen Kennedy. 2008. New Media's Potential for Personalization. *Information, Communication & Society* 11, 3, 307–325. http://doi.org/10.1080/13691180802025293

[39] Byungwan Koh. 2011. *User Profiling in Online Marketplaces and Security*. ProQuest LLC, Ann Arbor, MI.

[40] Bert-Jaap Koops and Ronald Leenes. 2014. Privacy Regulation Cannot be Hardcoded. A Critical Comment on the "Privacy by Design" Provision in Data-Protection Law. *International Review of Law, Computers & Technology* 28, 2, 159–171. http://doi.org/10.1080/13600869.2013.801589

[41] Nicole C. Krämer and Stephan Winter. 2008. Impression Management 2.0: The Relationship of Self-Esteem, Extraversion, Self-Efficacy, and Self-Presentation Within Social Networking Sites. *Journal of Media Psychology* 20, 3, 106–116. http://doi.org/10.1027/1864-1105.20.3.106

[42] Hanna Krasnova, Oliver Günther, Sarah Spiekermann, and Ksenia Koroleva. 2009. Privacy Concerns and Identity in Online Social Networks. *Identity in the Information Society* 2, 1, 39–63. http://doi.org/10.1007/s12394-009-0019-1

[43] Steffan Krüger and Jacob Johanssen. 2014. Alienation and Digital Labour—A Depth-Hermeneutic Inquiry into Online Commodification and the Unconscious. *tripleC* 12, 2, 632–645.

[44] D. J. Lair. 2005. Marketization and the Recasting of the Professional Self: The Rhetoric and Ethics of Personal Branding. *Management Communication Quarterly* 18, 3, 307–343. http://doi.org/10.1177/0893318904270744

[45] Marc Langheinrich. 2001. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. *Proceedings of the Third International Conference on Ubiquitous Computing*, Springer-Verlag, 273–291. Retrieved from http://www.vs.inf.ethz.ch/publ/papers/privacy-principles.pdf

[46] David Lazarus. 2015. Verizon's Super New Way to Mess with Your Privacy. *The Los Angeles times*.

[47] Yabing Liu, Krishna P Gummadi, Balachander Krishnamurthy, and Alan Mislove. 2011. Analyzing Facebook Privacy Settings: User Expectations vs. Reality. *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement*, ACM, 61–70.

[48] Michelle Madejski, Maritza Johnson, and Steven M Bellovin. 2012. A Study of Privacy Settings Errors in an Online Social Network. *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*, IEEE, 340–345.

[49] Alex Marthews and Catherine Tucker. 2014. Government Surveillance and Internet Search Behavior. *SSRN Electronic Journal*. http://doi.org/10.2139/ssrn.2412564

[50] Silva Martin and Stef Nicovich. 2013. Self Concept Clarity and its Impact on the Self-Avatar Relationship in a Mediated Environment. *Atlantic Marketing Association Conference Proceedings*.

[51] Viktor Mayer-Schönberger. 2009. *Delete: the Virtue of Forgetting in the Digital Age*. Princeton Univ. Press, Princeton, NJ.

[52] Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. 2008. Shining Light in Dark Places: Understanding the Tor network. *Privacy Enhancing Technologies*, Springer, 63–76.

[53] Soraya Mehdizadeh. 2010. Self-Presentation 2.0: Narcissism and Self-Esteem on Facebook. *Cyberpsychology, Behavior, and Social Networking* 13, 4, 357–364. http://doi.org/10.1089/cyber.2009.0257

[54] Edmund Mierzwinski and Jeffrey Chester. 2013. Selling Consumers Not Lists: The New World of Digital Decision-Making and the Role of the Fair Credit Reporting Act. *Suffolk University Law Review* 46, 3, 855–867.

[55] Hugh Miller and Jill Arnold. 2001. Self in Web Home Pages. In *Towards CyberPsychology*, Giuseppe Riva and Carlo Galimberti (eds.). IOS Press, Oxford, 73–94.

[56] Sayooran Nagulendra and Julita Vassileva. 2014. Understanding and Controlling the Filter Bubble through Interactive Visualization: a User Study. *Proceedings of the 25th ACM Conference on Hypertext and Social Media*, ACM Press, 107–115. http://doi.org/10.1145/2631775.2631811

[57] Nicholas Negroponte. 1996. *Being Digital*. Vintage Books, New York, NY.

[58] Donald A. Norman. 2002. *The Design of Everyday Things*. Doubleday, New York.

[59] OECD. 2013. *Exploring the Economics of Personal Data*. Retrieved June 23, 2015 from http://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en

[60] Bertell Ollman. 2001. *Alienation: Marx's Concept of Man in Capitalist Society*. Cambridge University Press, Cambridge; New York.

[61] Rolf Oppliger (ed.). 2014. *Secure Messaging on the Internet*. Artech House, Boston.

[62] Karl Palmås. 2011. Panspectric Surveillance and the Contemporary Corporation. *Surveillance & Society* 8, 3, 338–354.

[63] Michael Rader, A. Antener, Rafael Capurro, Michael Nagenborg, and L. Stengel. 2010. *D.3.2. Evaluation Report*. ETICA Project.

[64] Joel Reidenberg. 2005. Technology & Internet Jurisdiction. *University of Pennsylvania Law Review* 153, 1951–1974.

[65] Paul Resnick, R. Kelly Garrett, Travis Kriplean, Sean A. Munson, and Natalie Jomini Stroud. 2013. Bursting Your (Filter) Bubble: Strategies for Promoting Diverse Exposure. *Proceedings of the 2013 Conference on Computer Supported Cooperative Work Companion*, ACM Press, 95. http://doi.org/10.1145/2441955.2441981

[66] P.J. Rey. 2012. Alienation, Exploitation, and Social Media. *American Behavioral Scientist* 56, 4, 399–420. http://doi.org/10.1177/0002764211429367

[67] Jan-Willem van der Rijt. 2012. *The Importance of Assent: a Theory of Coercion and Dignity*. Springer, Dordrecht.

[68] George Ritzer. 2011. *Sociological Theory*. McGraw-Hill, New York.

[69] Ira S. Rubinstein. 2013. Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law* 3, 2, 74–87.

[70] Marisol Sandoval. 2012. A Critical Empirical Case Study of Consumer Surveillance on Web 2.0. In *Internet and Surveillance*, Christian Fuchs, Marisol Sandoval, Boersma Kees and Anders Albrechtslund (eds.). Routledge, New York, N.Y, 147–169.

[71] Kellyton dos Santos Brito, Frederico Araujo Durao, Vinicius Cardoso Garcia, and Silvio Romero de Lemos Meira. 2013. How People Care About Their Personal Data Released on Social Media. *Proceedings of 2013 Eleventh Annual International Conference on Privacy, Security and Trust (PST)*, IEEE, 111–118. http://doi.org/10.1109/PST.2013.6596044

[72] Amy J Schmitz. 2015. Secret Consumer Scores and Segmentations: Separating "Haves" from "Have-Nots." *Michigan State Law Review* 2014, 5, 1411.

[73] Bruce Schneier. 2015. *Data and Goliath: the Hidden Battles to Capture Your Data and Control Your World*. Norton, New York, NY.

[74] Richard C. Sherman. 2001. The Mind's Eye in Cyberspace: Online Perceptions of Self and Others. In *Towards CyberPsychology*, Giuseppe Riva and Carlo Galimberti (eds.). IOS Press, Oxford, 73–72.

[75] Daniel J. Solove. 2004. *The Digital Person: Technology and Privacy in the Information Age*. New York Univ. Press, New York, NY [u.a.].

[76] Inger L. Stole. 2014. Persistent Pursuit of Personal Information: A Historical Perspective on Digital Advertising Strategies. *Critical Studies in Media Communication* 31, 2, 129–133. http://doi.org/10.1080/15295036.2014.921319

[77] John Suler. 2004. The Online Disinhibition Effect. *CyberPsychology & Behavior* 7, 3, 321–326. http://doi.org/10.1089/1094931041291295

[78] Latanya Sweeney. 2013. Discrimination in Online Ad Delivery. *SSRN Electronic Journal*. http://doi.org/10.2139/ssrn.2208240

[79] Omar Tene and Jules Polonetsky. 2012. To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising. *Minnesota Journal of Law, Science & Technology* 13, 1, 281–358.

[80] Omer Tene and Jules Polonetsky. 2013. Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property* 11, 5, 239–272.

[81] Joseph Turow. 2011. *The Daily You: How the New Advertising Industry is Defining Your Identity and Your World.* Yale University Press, New Haven.

[82] Shaojung Sharon Wang. 2013. "I Share, Therefore I Am": Personality Traits, Life Satisfaction, and Facebook Check-Ins. *Cyberpsychology, Behavior, and Social Networking* 16, 12, 870–877. http://doi.org/10.1089/cyber.2012.0395

[83] Logan Danielle Wayne. 2012. The Data-Broker Threat. *Journal of Criminal Law and Criminology* 102, 1, 253–282.

[84] Alan F Westin. 1970. *Privacy and Freedom*. Bodley Head, London.

[85] S. Wilske and T. Schiller. 1997. International Jurisdiction in Cyberspace: Which States may Regulate the Internet? *Federal Communications Law Journal* 50, 119 – 178.

[86] Allen W. Wood. 2006. *Karl Marx*. Routledge, New York.

[87] Mike Z. Yao and Daniel G. Linz. 2008. Predicting Self-Protections of Online Privacy. *CyberPsychology & Behavior* 11, 5, 615–617. http://doi.org/10.1089/cpb.2007.0208

[88] G. I. Zekos. 2006. State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction. *International Journal of Law and Information Technology* 15, 1, 1–37. http://doi.org/10.1093/ijlit/eai029

[89] Shanyang Zhao, Sherri Grasmuck, and Jason Martin. 2008. Identity construction on Facebook: Digital Empowerment in Anchored Relationships. *Computers in Human Behavior* 24, 5, 1816–1836. http://doi.org/10.1016/j.chb.2008.02.012