Title: From Participatory Culture to Prosumer Capitalism: Imaginaries of Transparency in the Age of Corporate Surveillance

Bio: Pieter Verdegem is Assistant Professor (Tenure Track) in New media and Information & Communication Technologies in the Department of Communication Sciences at Ghent University, Belgium (pieter.verdegem@ugent.be).

Shenja van de Graaf is senior researcher and heads the 'Code, Commodification & the City' cluster at iMinds-SMIT, Vrije Universiteit Brussel, Belgium. Researcher at the London School of Economics and Political Science, UK. Honorary fellow at MIT Media Lab ID Hub, and a Futures of Entertainment fellow, USA (shenja.vandergraaf@iminds.be).

Abstract

In the complex ecosystem where community and technology intersect, social media data is playing a key role in the transition of social media platforms from a logic of sociability to one of commerce. Implicit in this transition are the issues of surveillance and transparency, as what started out as collective, user-centred social media platforms have become profit-driven organizations required to create commercial returns for investors. This contribution investigates the political economy of social media data, looking at how social media platforms are making this shift with new methods of surveillance to monetize user-generated-content and the personal information of users. With platforms such as Google, Facebook, and Twitter listed on the stock market, they are confronted with the continuous challenge of expanding their user base while also proving they can offer value for advertisers and other third parties. In trying to appeal to both users and investors, what is at stake is transparency, as users and other stakeholders are not made aware of what information exactly is being monetized and how surveillance techniques function in. This potentially undermines a transparent, effective, and trust-inducing interdependent relationship that underlies social media practices.

This contribution seeks to document and compare how Google, Facebook and Twitter present themselves to the world in the light of 'corporate surveillance'. By systematically analyzing their S-1 forms we uncover what information is disclosed about user surveillance, and how this is presented to users as well as to potential investors. Employing critical document analysis we investigate how and to what extent these platforms are transparent about their strategies of monitoring, mining and aggregating user data.

Theoretically, this contribution seeks to unpack how we have moved from participatory culture to a form of 'prosumer capitalism'. The first concept celebrates user expression and civic engagement in which prosumers are actively engaging in the production and distribution of content, thus feeling (socially) connected to others. The latter points at how the active role of users has resulted in a new form of capitalism, i.e. prosumer capitalism. In the social media era this means that the driving force behind the content shared on these platforms is not corporations such as Google, Facebook or Twitter, but is instead the users themselves. The relevant question then is whether corporate information informs users about their role in value creation, not only the presumption of content but also the social monitoring techniques that are built into these platforms.

Title: What should concern us about social media data mining's transformation of public space?

Bio: Helen Kennedy is Senior Lecturer in New Media in the Institute of Communications Studies, University of Leeds, UK (H.Kennedy@leeds.ac.uk)

Abstract

As social media usage grows, so too does the tracking, mining and analyzing of social media data. The rise of social media data mining has been driven by the increasing availability of data on users and their online behavior, as more social activities take place online; the decreasing cost of collecting, storing and processing data; and the exponential expansion of social media platforms from which much of this data is taken. Whilst more and more data is mined from a broad range of sources, social media data mining is of particular concern, because of the intimate place that social media occupy in people's lives and the intimate data that people share in social media spaces.

A number of criticisms have been leveled at social media data mining practices. First, it is characterized as a form of privacy violation. Social media spaces feel private, even if they are not, and people expect control over the flows of their personal information therein. The personal/private/intimate seeps into the public through social media data mining. Second, it's a form of surveillance. Social media data mining results in the emergence of new forms of surveillance (voluntary, self, lateral, as well as institutional and state) and the extension of governance beyond the public, into the personal/private/intimate (Trottier 2012). Third, it exploits the labour of social media users. Not only do data mining and related digital reputation building practices mean that users labour to turn themselves into commodities and self-brand, but these selves-as-commodities and the labour that underlies them are exploited by social media platforms for enormous profit (Fuchs 2013). Fourth, social media data mining is a form of algorithmic control; it results in social sorting. Individuals are categorized as targets or waste and if the latter, receive narrowed options – a form of social discrimination (Turow 2012) – and data is increasingly constitutive of culture, not just capturing culture, but feeding back into culture and having a shaping effect (Beer and Burrows 2013).

This paper surveys these critiques of social media data mining in order to ask what should concern us about social media data mining's transformation of public space. It proposes foregrounding debates about algorithmic culture and algorithmic control, to enable

more awareness and discussion of the less visible and more troubling ways in which social media data mining is transforming public space.

Title: Policing the Social Media. Control and Communication in a networked Public Sphere

Bio: Mirko Tobias Schäfer is Assistant Professor for New Media & Digital Culture at Utrecht University, The Netherlands (mts@mtschaefer.net / www.mtschaefer.net).

Abstract

For public administrations social media platforms appear as a new space to govern and to enforce laws. The platform providers have already put in place a number of tools and strategies to monitor user activities and user generated content. From automatic content screening over distributed flagging mechanisms to individual content moderation, platform providers make an effort to oust copyright violation and inappropriate content. They also provide commercially vast possibilities for third parties to monitor and evaluate social interaction and communication through their application programming interfaces. For law enforcement agencies the openly available communication of users, also dubbed open source intelligence, is a new source for crime detection. Several agencies have already set up units to patrol the social media precincts. The inherently marketeer-friendly social media platforms allow large scale analysis of data and provide for targeted advertising as well as for tracking individual users. As such they are well suited alike for marketing means and law enforcement.

This leads to several practices that transform our traditional understanding of private and public and the role of law enforcement in the public sphere. While death threads had to be reported by the potential victim, now the police intercepts such messages when distributed through social media and might take action when considered necessary. Through social media the police communicates differently with citizens and invites their participation in reporting crime, providing information or spreading police communication. The monitoring of activist communication in platforms such as Facebook, Twitter and YouTube expands traditional forms of infiltration and surveillance. The analysis of social graphs, personal social media profiles and timelines raises issues of privacy and legitimacy of security demands.

This paper revisits practices of social media use and monitoring by police forces. Findings result from an analysis of monitoring tools and practices as well as from an investigation into law enforcement's take on social media in the Netherlands. This paper discusses the emergence of security dispositives in the political economy. With reference to Foucault's notion of governmentality, monitoring tools and practices of policing social media will be discussed as “mechanisms of security.” In their co-production of security, this

assemblage of private monitoring companies and public law enforcement authorities raise serious issues of accountability and civic liberties.

Title: Privacy, Data Security, and the Public Spaces of Social Media

Bio: Jennifer Holt is an Associate Professor of Film and Media Studies at the University of California, Santa Barbara, USA. Director of the Carsey-Wolf Center's Media Industries Project at UCSB (jholt@filmandmedia.ucsb.edu).

Abstract

As digital content distribution and engagement with social media platforms becomes increasingly reliant on streaming platforms, remote servers and access to viewers' preferences, privacy and data security have become key issues for producers, distributors, and consumers of cloud-based media and social networking sites. The necessity for securely managing digital identity and maintaining the confidentiality of online data has become vital for governments, individual citizens, and private corporations. The international nature of cloud storage makes this challenging, given the gaps/fissures in international data jurisdiction, regulating third party hosts, and the global difficulties defining "personal information." This presentation focuses on the role that privacy and data security are playing in big data-driven digital content distribution and social media platforms.

The focus lays on a comparative analysis of US and European approaches to privacy that impact content providers in a digital era of streaming media and connected viewing, delineating current boundaries (legal, psychological, practical) for using digital data. European national initiatives, such as those in Germany and Switzerland, aim to create insular cloud infrastructures. These are contextualized within the EU's impending Connected Continent initiative, which advocates implementing data privacy laws that will foster a single interoperable market with high data portability. The US is embracing more market-driven approaches which include the creation of a new Identity Ecosystem, a competitive market of identity service providers (the *new* ISPs).

As comparative case studies, the EU Connected Continent initiative and the US Identity Ecosystem reveal four conceptual dimensions of privacy regulation currently under contestation: interoperability, security, identity, and data flow. The EU seeks to protect identity with a portability law that gives consumers the right to move personal information among data controllers, while the US supports the market-driven innovation of identity management systems. Contested understandings of data flow affect rules governing bandwidth management and user monitoring, including techniques like deep packet

inspection, with the EU favoring neutral conduits in their legislation and the US backing existing techniques of traffic-management.

The possible relationships among the dimensions provide a conceptual matrix of privacy, and international privacy regulation. It informs culturally specific responses to data mining and network analytics, such as the advocacy of "the right to be forgotten." This consumer movement seeks to instantiate privacy protections precisely by defining privacy in the negative. It promotes the absence of "big data" related to individuals, straddling the competing models of privacy that the Connected Continent and Identity Ecosystem respectively represent.