

Vol. 19 (07/2013)

Reputation in the Cyberworld

edited by Michael Eldred

Editor of this issue:

Michael Eldred

artefact text & translation, Cologne, Germany

Editors of IRIE

Prof. Dr. Rafael Capurro (Editor in Chief),
International Center of Information Ethics (ICIE)
Redtenbacherstr. 9, D-76133 Karlsruhe, Germany
E-Mail: rafael@capurro.de

Prof. Dr. Johannes Britz,
University of Wisconsin-Milwaukee, USA and
University of Pretoria, South Africa
E-Mail: britz@uwm.edu

Prof. Dr. Thomas Hausmanninger,
University of Augsburg, Germany,
Universitätsstr. 10, D-86135 Augsburg
E-Mail: thomas.hausmanninger@kthf.uni-augsburg.de

Dr. Michael Nagenborg,
IZEW, University of Tübingen,
Wilhelmstr. 19, D-72074 Tübingen, Germany
E-Mail: michael.nagenborg@izew.uni-tuebingen.de

Prof. Dr. Makoto Nakada,
University of Tsukuba, Japan,
Tennodai, Tsukuba, 305-8577 Ibaraki
E-Mail: nakadamakoto@msd.biglobe.ne.jp

Dr. Felix Weil,
QUIBIQ, Stuttgart, Germany,
Heßbrühlstr. 11, D-70565 Stuttgart
E-Mail: felix.weil@quibiq.de

Vol. 19 (07/2013)

Content:

Editorial:

On IRIE Vol. 19 1

Michael Eldred:

Introduction to Reputation in the Cyberworld 2

Michael Eldred:

Reputation in the Cyberworld 4

Stefano De Paoli:

**The Automated Production of Reputation: Musing on bots and the future of reputation
in the cyberworld 12**

Daniel Nagel:

The Quest for a Clean Slate Building and Protecting Reputation in the Cyberworld 22

Anna-Maria Piskopani:

Ethical considerations on "refreshing" digitized reputation by changing one's name 32

Bo Zhao:

An Analytical Note: How the Internet Has Changed Our Personal Reputation 39

Gloria Kirwan, Conor Mc Guckin:

Professional Reputation and Identity in the Online World 47

Yohko Orito, Kiyoshi Murata and Yasunori Fukuta:

Do online privacy policies and seals affect corporate trustworthiness and reputation? 52

Ulrik Franke:

On the cyber-reputation of governments 66

Editorial: On IRIE Vol. 19

What is the **reputation of IRIE**? How can it be measured? There are, of course, the classical techniques to assess the reputation of a scientific journal: mainly by indices it is listed in, citation indices, the TSI, but also the price tag of an issue and of course the reputation of its authors, editors, etc. They are all widely used in this regard but still, they all stem from the Gutenberg Galaxy, so the question remains: Are they still valid in the cyberworld, valid for a scientific online journal focused on a very special, very innovative area of expertise?

Could the indications of reputation in the cyberworld (in fact, they also enjoy a rather classical status by now) be of any help:

- **Ranking in google?** In fact, we are # 2 for the keyword "information ethics" - out of 192,000,000 after all (as of 23rd July 2013) - but still second to Wikipedia. Does this mean the entry on "information ethics" in Wikipedia deserves a higher scientific reputation than IRIE?
- **Number of visitors to the web-site?** We can proudly state that the counter shows more than 83,000 visits (also as of 23rd July 2013) and still counting. That's a rather large number for a scholarly journal. Still, there are some web-sites with far more visitors that without any doubt would be assigned a much lower scholarly reputation than IRIE!
- **Number of back-links, comments, tweets, etc.?** Do they or a mixture of all of them (by the way the latter would finally lead to the ranking in google again if all these ingredients are put together into a proper formula) correctly reflect the scholarly quality of IRIE in the cyberworld?

Indeed, the question about how to assess the scholarly reputation of an online journal such as IRIE is not yet answered. And precisely that is reason enough for us to raise this very question in an issue of IRIE – of course on a more conceptual level, not necessarily narrowed to the assessment of the reputation of IRIE itself.

Thanks to Michael Eldred's solid work, we received some very illuminating and inspiring contributions on this subject. And yet, only one thing is certain: To the degree this issue contributes to raising if not solving the question of reputation in the cyberworld, it contributes also to the reputation of IRIE in the cyberworld - as well as in the world in general and the scholarly world in particular. So please, see for yourself! There's good reason that in philosophical discourse this latter is the only thing that counts.

Sincerely yours,

the editors.

Michael Eldred:

Introduction to Reputation in the Cyberworld

Reputation is a very familiar phenomenon. Your reputation is who you are held to be by others; it is your social standing. A good reputation is helpful for getting through life, and, in one sense or another, is indispensable for rising through the social ranks. For some career paths, notoriety may actually boost your standing in the world. Your reputation precedes you as the information or narrative in circulation about who you have been, so there is an undeniable connection to the temporal dimension of the past. Your very identity is tied to the reputation you have established or ruined in your personal social world.

In business transactions reputation can play a crucial role, especially where credit is required to finance them. A creditor has to trust a potential debtor, thus giving him credit in the double sense. Whether we trust each other in any kind of social interplay depends on each other's reputations in circulation that have come to our ears. Reputations apply to both natural and juridical persons. Any corporate entity will be jealous of its reputation because it has a direct link to commercial success. The growing phenomenon of Corporate Social Responsibility evidences how important a company's standing in the community and society has become, including for the bottom line. Companies' reputations have long since been drawn into political struggles over fair corporate practices.

The internet has been a game-changer in opening up an entirely new, artificial, digital world - the cyberworld - in which reputations of persons and companies circulate, reified as bit-strings. Your very identity - who you are - is today tied to bit-strings in circulation that have some connection to your proper name. Hence the desire of some to hide their identity in the cyberworld by means of pseudonyms or anonymization, whereas for others, the cyberworld provides an unprecedented opportunity for showing off who they are and launching their reputation more widely, even worldwide. The ease with which bit-strings relating to personal identity can be brought into circulation in the global digital matrix allows reputations and even fame to be promoted without the backing of specific media corporations. These used to function as gatekeepers who assessed whose reputation was worthy of dissemination and whose was not. Similarly, companies now employ the cyberworld to advertise not just products and services, but to promote who they are. Even name- or brand-recognition is a vital component of commercial success. Only because company names and brands are intimately linked to reputation are they so jealously guarded. The cyberworld opens a new arena for debating companies' reputations and social standing.

Questions raised include:

How does digitized reputation relate to 'normal' reputation, to human freedom? to truth? to rhetoric?

Will the loss of digitized reputation, or the failure to establish one, amount to a kind of social death, of social non-existence in our brave new cyberworld?

Is the possibility - and thus power - of talking about someone in the third person a fundamental form of social violence and of the ineluctable social power play?

How is the striving to establish a reputation related to the will to power?

How can reputation be damaged by and how can it be protected against slander, libel, calumny, rumour and the like? How are these latter phenomena to be characterized? Are only legal means available to protect reputation?

How are personal reputation and corporate reputation different?

Do online social media enhance or impede, further or endanger the establishment of personal reputation?

Do pseudonyms in the cyberworld (legitimately?) enable flexible and/or multiple reputations - versatile plays with masks of identity?

How does reputation provide a lever for achieving a fair power play in civil society?

Who has control over my reputation in the cyberworld, if bit-strings 'never die' and companies gather and store my personal digital trace? Is my cyber-reputation inescapable?

How do companies' strategies to establish and enhance reputation via Corporate Social Responsibility offer also a point of attack in the power play of civil society to make companies change corporate policies and practices?

Can public debate in the cyberworld over a company's reputation serve to constrain corporate practices in lieu of legal frameworks that have trouble being enforced on a global level?
How does the phenomenon of reputation change across cultures and how do the rules of play for establishing or losing reputation shift?

The present thematic issue of IRIE on *Reputation in the Cyberworld* presents a range of articles from various disciplines, countries and perspectives which touch upon, directly or indirectly, some of the questions posed above. I think each of these peer-reviewed articles speaks for itself.

Michael Eldred:

Reputation in the Cyberworld

Abstract:

The article explores the socio-ontological foundations of the phenomenon of reputation in the context of today's ever-encroaching cyberworld. The categories of whoness and value are essential for understanding reputation ontologically. The cyberworld itself has only become historically possible through the Cartesian mathematical cast of being and its digital refinement in the Universal Turing Machine. From one perspective, the cyberworld is an endless concatenation of Turing machines. It is, however, also a matrix in which bit-strings circulate that have a decisive impact on who anybody is held to be by others, i.e. on their reputation. The game of striving to be esteemed as who you are thus assumes a new complexion in the digital era.

Agenda:

Who you are	6
Estimating, esteeming, evaluating, valuing who you are	6
The power play of who-estimation.....	7
Digitized identity	7
What is the cyberworld?	7
Calculability of bit-string identity	8
Striving to be somewho in the cyberworld.....	9
Vicissitudes of reputation in the cyberworld	9
Personal reputation	9
The value of corporate reputation	10
Goodwill: how a company is evaluated	10

Author:

Dr. Michael Eldred:

- artefact text & translation, Antwerpener Str. 1, D-50672 Cologne, Germany
- ☎ +49 - 221 - 9520 333 ✉ me@arte-fact.org 🌐 www.arte-fact.org
- Relevant publications:
 - *Digital Whoness: Identity, Privacy and Freedom in the Cyberworld* (with R. Capurro & D. Nagel) Frankfurt: ontos verlag 2013, 312 pp.
 - *The Digital Cast of Being: Metaphysics, Mathematics, Cartesianism, Cybernetics, Capitalism, Communication* Frankfurt: ontos verlag 2009, 137 pp.; emended, revised and extended e-book edition, Version 3.0, 2011 215 pp. available at www.arte-fact.org

- *Social Ontology: Recasting Political Philosophy Through a Phenomenology of Whoness* Frankfurt: ontos verlag 2008, xiv + 688 pp.; second revised, emended and extended e-book edition, Version 2.1 2011, 785 pp. available at www.arte-fact.org

This article offers some fundamental philosophical clarification of reputation on the basis of a phenomenology of whoness. The ontology of the cyberworld will be sketched, and the phenomenon of reputation, both personal and corporate, situated within this context.¹

Who you are

Who are you is not a trivial question. It is a socio-ontological question concerning your presencing and absencing in the time-clearing of the world. Who you are, is said here in the second grammatical person, who I am, is said in the first person, who he or she is, is said in the third person singular, and who they are, is said in the third person plural. These grammatical persons, too, are not trivial taxonomic matters of grammar; rather, each is a phenomenon of presencing in its own right calling for reflection. The question concerning who you are is to be distinguished from the traditional metaphysical question as to *what* something is, posed in the third person singular. Whereas the question concerning whatness (essence, quiddity, substance) has a venerable history going all the way back to Plato and Aristotle, the explicit, emphatic question concerning whoness (quissity) is relatively recent, arising in the wake of Ludwig Feuerbach.² Martin Heidegger brings in a new twist by explicitly posing the question concerning whoness (Wersein, Werheit) in the 1920s,³ which in turn was taken up in a different vein by Hannah Arendt in her opus magnum, *The Human Condition*⁴ and also by myself, again in a different vein, in various works.⁵

Heidegger uncovered the underlying meaning of being implicit throughout Western thinking to have been presence. To be who you are is to be present in the world, which is itself fundamentally temporal, namely, the three-dimensional time-clearing of past, present and future in which you present and absent yourself, showing yourself off *as* who are, including also privative modes of concealing (certain aspects of) who you are. In the case of whos, presence in the world is always also a self-presenting, of showing-off.

Estimating, esteeming, evaluating, valuing who you are

It is essential for showing-off to have yourself acknowledged by others *as* who you show yourself to be. You choose, or neglect to choose, your masks for self-display in adopting this or that behaviour and views, wearing certain clothes rather than others, etc. The interplay with each other is always a reciprocal *estimating* of each other's self-presentations. You present yourself as some who or other, thus making a certain *impression* on others. Who you *are* is always a matter of having adopted certain *masks of identity* reflected from the world as options for who you could be in the world. Each human being is an *origin* of his or her own self-movements and has an *effect* on the surroundings, changing them this way or that, intentionally or unintentionally. Being estimated positively in presenting yourself to others is the phenomenon of *esteem*. Such esteeming, evaluating estimation of your self-presentation depends also on presenting, or at least seeming to present, yourself as a *capable* who in some sense or other, which will be estimated variously in different circles and situations.

¹ This article draws on my contributions to Capurro/Eldred/Nagel 2013.

² And on through authors such as Martin Buber, Eugen Rosenstock-Huussy, Ferdinand Ebner, Eberhard Grisebach, Karl Heim, Gabriel Marcel, Friedrich Gogarten, Helmut Plessner, Adolf Reinach, Dietrich von Hildebrand, Wilhelm Schapp, Alfred Schütz, Ludwig Binswanger, Karl Löwith, Hermann Levin Goldschmidt and Emmanuel Lévinas; cf. Theunissen, Michael 1977 for a comprehensive overview of most of these authors.

³ Cf. e.g. Heidegger, Martin 1927, 1975.

⁴ Arendt, Hannah 1958.

⁵ Eldred, Michael 1989, 1999, 2008.

The power play of who-estimation

The core mask of identity borne by a who is one's own *proper name*, around which other masks cluster. Above all, it is a matter of adopting masks of *ability* reflected by the world, thus developing your own potential abilities into developed personal *powers* of whatever kind. Each who ends up in some vocation, profession, job, social role or other, thus becoming who she or he is in living that cast role, and this is the mask of identity that *somewho*, for the most part, presents to the world *as who* he or she is, being estimated and esteemed by the others in the interplay. Since human beings are estimated and esteemed as who they are above all on the basis of their personal *powers and abilities*, and because the exercise of such powers also effects some change or other in the world, the interplay of mutual estimation is always also a *power play*, especially in the sense of mutually estimating each other's who-status. At first and for the most part, you wish to have your developed powers and abilities, whatever they may be, esteemed by the others in the power play. You may *fail* in doing so. In sharing the world, human beings are constantly estimating and evaluating each other's performances in presenting themselves *as* *somewho* or other through their powers and abilities, i.e. their *merit*, as that which deserves esteem. Those of a similar who-standing are therefore, for the most part, in a *competitive rivalry* with one another.

The individual powers and abilities you have adopted as masks of identity widens the focus from the temporal mode of presence because such powers refer both to who you have already become and also to who you may become in future. The estimation of your abilities by the others gives rise to your *reputation* as who you are, and reputation refers to how you have presented yourself to the world in the past, which is never past, because you have inevitably always already established or ruined your reputation as who in some circle or other. Conversely, who you will become depends crucially also on your potential being estimated by those who are in a position (especially parents and teachers) to foster the development of that potential to powers and abilities that an individual *actually has* at its disposal. Furthermore there is the *futural* aspect of whoness in the *ambition* that you have to be cast in a certain who-role, usually by honing your abilities of whatever kind. Such ambition is always also linked to *as* who you want to be regarded in the world and is thus tied intimately to the power play of mutual estimation. Ambition is the striving to leave your mark on the world, even to the point of establishing your *fame* as someone about whom the 'world' speaks. Leaving your mark on the world is a way of making an impression on the shared world, namely, a *lasting* impression, which again refers to the temporal dimension of the past or 'beenness'.

Wanting to make any impression at all on the world, let alone, wanting to have an impact or to leave your mark on the world, are all manifestations of the *will to power to be who*. To be *somewho* in the world amounts to having your self-presentation to the world estimated, esteemed and reflected by the world, to *come to stand* in shared presence as a who with some standing. Such *standing presence*, however, is very fragile in the power play of togetherness in general, for it depends on the mirror game of mutual self-presentation in which having a stand as who depends on the reflections of estimation received back from the others. Appreciative reflections of esteem from the others may be very fickle, easily replaced by depreciative, even downright derogatory, reflections. This contrasts with traditional metaphysical determinations of whatness which is a standing presence either in the sense of possessing an enduring, well-defined essence, or in the sense of possessing an underlying, enduring substance that persists in presence. Whoness as a mode of presencing is the way in which human beings share a world with each other, i.e. the mode of mutually mirroring togetherness in the time-space of the world. Such presencing as *somewho* in an ongoing power play of mutual estimation is insubstantial, that is, lacking an underlying substrate, and is thus *groundless*.

Digitized identity

What is the cyberworld?

Cyberworld is the name not for some merely ontic-factual, artificial thing, but the existential-ontological name for the ontic-factual internet plus other interlinked networks *insofar as* this global technical thing also represents

an (electromagnetic) *medium for the movement of digital beings* (bit-strings) in which we human beings participate and through which we also steer, either directly, or indirectly through automatically executable digital code. This gives rise, say, to the possibility of robots, which are artificially 'animated' machines that, once programmed, have the source of movement within themselves, even though they need a current of electrons to drive them.

The cyberworld, as the materialization of the digital cast of being,⁶ is an artificial world produced by outsourcing the arithmologos as (executable, automatic) digital code that moves in its own global medium. It is populated by countless trillions of bit-strings that are either 'passive' digital data or 'active' executable program code. These two kinds of code copulate with each other in countless billions of Universal Turing Machines,⁷ generating new bit-strings that continue to circulate throughout the cyberworld, which itself is nothing other than a never-ending concatenation of Universal Turing Machines impregnated in the electromagnetic matrix. Digital beings are nothing but digital code, i.e. strings of bits. A bit is pure binary difference that can be represented by, say, 1 and 0. To write a bit, a stable difference in the inscription matrix between two unambiguous states is required, and this is provided by electromagnetic states of the medium that can be changed in a controlled way by electromagnetic force fields, including currents of electrons, photons or laser beams. Digital program code must be 'legible' to a processor as a set of step-by-step instructions (the algorithm) about what to do with digital data input. After processing, other bit-strings are output, which are signals sent to destinations to trigger electromagnetic effects.

As far as the human user or denizen of the cyberworld is concerned, the cyberworld presents itself to him or her through the various interfaces that today have been well-adapted to the human body and mimic the physical world. Such interfaces are technical, requiring a technical device of some sort: desktop, laptop, hand-held, implanted chip or whatever. This device itself is assigned a number automatically (e.g. IP address) by the cyberworld; it is identifiable through this number, which may be combined with other numbers such as location and time co-ordinates. The human user of a digital device interfaced with the cyberworld is willy-nilly identified with this device's number so that, in a certain way, the user's identity itself becomes this number as far as his or her presence in the cyberworld goes. A cyberworld denizen can call up data from all over the world, according to his or her interests, which are a reflection of personal identity, i.e. of who this individual understands him- or herself to be in the world. A cyberworld denizen can also present him- or herself as who s/he is by posting data at some site within the cyberworld. These data, of whatever kind (text, image, sound, video) are *identified* with the individual posting them, who may or may not use a pseudonym.

Calculability of bit-string identity

Because all sorts of data circulating in the cyberworld can easily be stored, i.e. recorded automatically, this opens up many opportunities for processing those data, in particular, with a view to establishing the identity of a particular user and his or her life-movements. The individual is identified with a piece of code (an IP address, the ID of a digital device, etc.) that enables also cyber-surveillance and cyber-tracking, amounting to 'überveillance'.⁸ All the digital data in the cyberworld relating to a certain individual can be pieced together, through the appropriate executable code, in an individual profile that inverts the first-person perspective of what someone does in the cyberworld into a third-person perspective of a reified digital data profile through which others, in a certain way, have disposal over who the individual concerned *is*. The cyberworld is a cyber-space-time with digitized Cartesian space-time co-ordinates recording movements within it, and not the time-clearing of a world in which human being exists ec-statically stretched toward three independent temporal dimensions.⁹ Hence the third-person, 'objective', 'scientific' view of an individual that is enabled through the linking of digital data,

⁶ Cf. Eldred 2009/2011.

⁷ Cf. Eldred 2012a.

⁸ Cf. Michael & Michael 2010.

⁹ Cf. Eldred 2009/2011 for more on three-dimensional, ecstatic time.

clashes with the first-person view of an individual living his or her life in and out of the cyberworld or the first-and-second person viewpoints of sharing a world.¹⁰

Striving to be somewho in the cyberworld

The striving of any who to be somewho in the cyberworld is to receive as much *appreciative feedback* from other cyberworld denizens as possible, which can happen fairly directly due to the cyberworld's accessibility to everybody. In the case of other public media, there is usually a gatekeeper that watches over who is to have a say, to make an appearance in that medium. The who-game thus comes to be played on a larger, global, digitally mediated scale, a cyber-stage. Nevertheless, the stakes remain, firstly, being noticed at all, and, secondly, gaining others' attention, being esteemed and estimated highly by others (positive feedback). What Plato called 'love of esteem' thus takes on a different garb in a different scenario in the digital age, but remains the same in that it is still the who-game which, of course, is played not only in the West. The lure of being esteemed as somewho is amplified by the ease of self-presentation in the cyberworld.

Another aspect of finding one's self in the cyber-era is that, due to its global reach, the cyberworld reflects many different possibilities of living in the world, from all the world's different cultures. Ease and cheapness of access to the internet for billions of people open up a vast space in which to find one's self, thus perhaps causing friction with the expectations within the ethos of a given culture. Especially entertainment media such as film and music proffer identity masks to anyone who'll put them on, adopting a life-style and self-understanding that may be promoted by a culture industry. The ease with which digital beings disseminate throughout the cyberworld leads to a fast merging of possible identities, especially for youth who are still finding themselves, also in what the cyberworld offers by way of quickly circulating identity masks that inevitably induce also a certain levelling of youth-identity. One of the more trivial of such masks is fashion, i.e. how somewho dresses to present him- or herself to the world. With the cyberworld, youth fashion especially spreads very quickly around the globe, with youth fashion strategies demarcating who one is from one's parents' identities becoming adopted rapidly. The typical different local cultural identities also become more visible in their differences via the cyberworld.

Vicissitudes of reputation in the cyberworld

Personal reputation

With the digitization of identity in the cyberworld, one could say that the genie is out of the bottle. Once who you are has become a set of bit-strings circulating in the global electromagnetic medium, who you are held to be by others, i.e. your reputation, becomes a matter of interpreting and evaluating those bit-strings identified with you. These identity bit-strings are the traces of your presence and movement through the cyberworld, and these traces *remain* — unlike many traces of your life-movements in the physical world — and *accumulate* in the electromagnetic matrix. Such digital traces, in turn, can be gathered and processed by other bits of executable digital code, i.e. they can be input into yet another Turing machine which mines those data either generally or specifically. Market research, for instance, is interested in mining personal data for the sake of assessing your potential as a consumer in a certain market segment, whereas a prospective employer may be interested in your personal reputation as represented by your cyberworld presentation of yourself over time. In particular, your vocational reputation as presented by circulating bit-strings will influence how potential customers and clients will evaluate you, or whether a potential employer will hire you. No bit-string with an identity-link to you is therefore innocent, and its longevity in the cyberworld means that it may be taken up and re- and misinterpreted in later contexts. After all, who you are and held to be by others is always a matter of interpretation in which certain bit-strings are understood *as such-and-such*, i.e. the *hermeneutic As* is always

¹⁰ Cf. Capurro 2011.

operable. Via stored bit-strings, your identity from the past may be resuscitated with either beneficial or deleterious, fair or unfair results. The options for recasting yourself at a later stage of life after your past reputation has been 'forgotten' alter with the calculating potentials of the cyberworld that retrieves with ever more powerful executable digital code who you have been.

With the onset of the cyberworld, who you are in the world, i.e. your being, becomes an *identity* with something *different* from you, namely, a certain set of bit-strings circulating in the interconnected global electromagnetic medium, whose interpretation amounts to the third-person reputation you have in the world as a whole. This is a qualitatively new level of *reification* of your reputation beyond the estrangement from your personal identity already introduced with the advent of mass media in the 19th and 20th centuries. Who you are held to be, and consequently, how you are esteemed and valued, becomes in part a function of how certain bit-strings are interpreted and evaluated. In certain cases it may become necessary for you to defend yourself legally, so far as possible, against libel, slander and calumny that denigrate your who-status. In this way, you may even be drawn into Joseph K.'s nightmare as Kafka eerily unfolds in *The Trial (Der Prozeß)*, which opens with the line:

*"Someone must have slandered Joseph K., for one morning, without his having done anything bad, he was arrested."*¹¹

The value of corporate reputation

The dimensions of the reification of reputation expand when considering non-natural, juridical persons, including commercial companies. Any corporate entity will be jealous of its reputation because it has a direct link to commercial success. The growing phenomenon of Corporate Social Responsibility evidences how important a company's standing in the community and society has become, including for the bottom line. Companies' reputations have long since been drawn into political struggles over fair corporate practices. This is well-known and the stuff of daily news. But what are the socio-ontological underpinnings of this now familiar phenomenon? The crux is that a juridical person such as a commercial company is not merely a what that can be considered simply as an organization in terms of, say, its efficiency, but a who. Whoness as a fundamental socio-ontological category is tied to value, esteem, estimation (timh/), i.e. to phenomena already central for Plato and Aristotle and then throughout the Western tradition.¹² The essential feature of a capitalist economy is that it is mediated through and through by the movement, the circulation of reified value that, in this movement, successively assumes and strips off various value-forms such as commodities, money, productive capital, loan-capital. Through an *augmentative* circulation of value, each and every commercial enterprise is out for gain. The essence of capitalist economy can therefore be termed the "gainful game".¹³

Goodwill: how a company is evaluated

A capitalist enterprise is valued not only via the commodity goods and services it offers on the market, but also through its corporate reputation as a profit-making entity. How a company is perceived, i.e. estimated and esteemed, in the public domain affects also how well it does in gainful activity. Moreover, any going concern well-established in the market-place has a reputation which, as fictitious capital,¹⁴ has a certain value that can even be monetized, i.e. transformed into reified value, upon selling the company. This value-portion is the company's *goodwill*, which is estimated regularly in the company accounts and realized when the company is merged or acquired. Apart from this, any company listed on the stock exchange is factually valued every day and every second by its market capitalization which is affected, among other things, by the news-feed about

¹¹ "Jemand mußte Josef K. verleumdet haben, denn ohne daß er etwas Böses getan hätte, wurde er eines Morgens verhaftet." Kafka 1958 p. 7.

¹² Cf. for details Eldred 2008/2011 esp. Chaps. 2 and 5.

¹³ Cf. for details Eldred 2000/2010 esp. Chap. 7.2.

¹⁴ Cf. for details Eldred 1984/2010 § 20 'The Firm as Fictitious Capital. Goodwill'.

the company's activity, including those that enhance or depreciate its corporate reputation. For instance, negative news-feed about a multinational's supply-sourcing in a developing country can greatly damage corporate reputation and hence also market capitalization. The company's economic goodwill diminishes. Thus, a company's who-status, too, has a reified value that is constantly being evaluated by the stock market as a whole, and this reified stock-market evaluation depends also on the good will exhibited toward the company in the public domain. The cyberworld with its circulating bit-strings relating to a given company and its activities, its market strategies, corporate policies, etc. today has a decisive impact on corporate reputation. No company of any size can afford to ignore how it is held to be, and thus estimated and evaluated, by the flow of bit-strings pertaining to it. This calls forth the necessity of measures to enhance and defend corporate reputation, such as public relations officers, corporate philanthropic activities, corporate governance policies and statements, etc. Thus even, and especially, huge and mighty companies are drawn into and subjected to the evaluations coursing through the cyberworld.

References

- Arendt, Hannah *The Human Condition 2nd ed. with an introduction by Margaret Canovan, Chicago U.P. 1998, 1st ed. 1958.*
- Capurro, Rafael 'Never Enter Your Real Data' *International Review of Information Ethics Vol. 16 2011 pp. 74-78.* URL: www.capurro.de/realdata.html
- Capurro, Rafael, Michael Eldred & Daniel Nagel *Digital Whoness: Identity, Privacy and Freedom in the Cyberworld Frankfurt: ontos verlag 2013.*
- Eldred, Michael *Critique of Competitive Freedom and the Bourgeois-Democratic State: Outline of a Form-Analytic Extension of Marx's Uncompleted System Copenhagen: Kurasje 1984, e-book edition www.arte-fact.org 2010. With an extensive bibliography.*
- Eldred, Michael *Der Mann: Geschlechterontologischer Auslegungsversuch der phallogischen Ständigkeit Frankfurt: Haag + Herchen 1989.*
- Eldred, Michael *Phänomenologie der Männlichkeit: kaum ständig noch Dettelbach: Röhl 1999; e-book edition www.arte-fact.org*
- Eldred, Michael *Kapital und Technik: Marx und Heidegger Dettelbach: Röhl 2000; english version in Left Curve No. 24, May 2000; www.arte-fact.org Ver. 3.0 2010.*
- Eldred, Michael *Social Ontology: Recasting Political Philosophy Through a Phenomenology of Whoness Frankfurt: ontos 2008; 2nd emended, revised, extended e-book edition www.arte-fact.org 2011. With an extensive bibliography.*
- Eldred, Michael *The Digital Cast of Being: Metaphysics, Mathematics, Cartesianism, Cybernetics, Capitalism, Communication Frankfurt: ontos verlag 2009, 137 pp.; emended, revised and extended e-book edition, Version 3.0, 2011 www.arte-fact.org With an extensive bibliography.*
- Eldred, Michael *Out of your mind? Parmenides' message www.arte-fact.org Ver. 1.0 2012.*
- Eldred, Michael 'Turing's cyberworld of timelessly copulating bit-strings' www.arte-fact.org Ver. 1.0 2012a.
- Kafka, Franz *Der Prozeß Frankfurt: Fischer 1958.*
- Heidegger, Martin *Sein und Zeit Tübingen: Niemeyer 1927, 15th ed. 1984.*
- Heidegger, Martin *Die Grundprobleme der Phänomenologie Marburger Vorlesung SS 1927 Gesamtausgabe Band 24 (GA24) ed. F-W. v. Herrmann, Frankfurt/M.: Klostermann 1975 English translation: The Basic Problems of Phenomenology Indiana U.P. 1982.*
- Michael, G.M. & Katina Michael 'Toward a State of Überveillance?' *Technology & Society Vol. 29 No. 2 2010 pp. 9-16.*
- Theunissen, Michael *Der Andere: Studien zur Sozialontologie der Gegenwart 2nd ed. Berlin/New York: W. de Gruyter, 1977.*

Stefano De Paoli:

The Automated Production of Reputation: Musing on bots and the future of reputation in the cyberworld

Abstract:

Reputation is considered as the summary of a person's relevant past actions in the context of a specific community and is a concept which has gained huge relevance in the cyberworld as a way of building trust. Increasingly, however, reputation is awarded to users after they have carried out repetitive, mechanical or trivial actions. This opens the space to a phenomenon which we can define as the automated production of reputation: reputation produced by the means of software technologies known as bots that can easily automate repetitive online actions. In this paper the phenomenon of automated production of reputation is preliminarily defined and presented using three different empirical examples: Massively Multiplayer Online Games, the social network twitter and the reputational hub Klout. The paper also discusses some of the foreseeable negative consequences of the automated production of reputation and in particular the risks related to the loss of trust in online communities.

Agenda:

Introduction	13
Reputation in Context	13
The Automated Production of Reputation	15
Example 1: Massively Multiplayer Online Games	16
Example 2: Fake followers on twitter	17
Example 3: Klout Manipulation	18
Discussion: Automated Production of Reputation and its Consequences	19
Conclusion: What's next?	20

Author:

Dr. Stefano De Paoli:

- Fondazione <ahref, Vicolo Dallapiccola 12, 38122, Trento, Italy
- ☎ + 39 - 0461 - 235794 , ✉ stefano@ahref.eu stefano.depaoli@gmail.com
- Relevant publications:
 - De Paoli Stefano and Kerr Aphra. On Crimes and Punishments in Virtual Worlds: bots, the failure of punishment and players as moral entrepreneurs. *Ethics & Information Technology*, 14(2): 73-87, 2012.

Introduction

There is a phenomenon which will have an increasing relevance for the future of reputation in the cyberworld: *the automated production of reputation*. In this position paper I will define it, reflect on it using empirical examples and make some preliminary observations on some problematic issues related to it.

Reputation is considered as the summary of a person's relevant past actions in the context of a specific community and is a concept that has gained huge relevance in the cyberworld as a way of building trust. Some authors even see online reputation as the central aspect of contemporary digital society and talk about "The Reputation Society" (Masum and Tovey, 2012). In the cyberworld, reputation is "created" and "disseminated" by the means of technological systems known as reputation systems (Dellarocas, 2012). Increasingly, however, in these systems, reputation is awarded to users after they have carried out repetitive, mechanical or trivial actions. An immediate example would be awarding simple "likes" to a fan page on Facebook¹⁵ (an action that simply requires the repetitive clicking of a button on the interface).

Generally speaking, repetitive and mechanical actions are often automated with technologies. An example we can think about is repetitive actions carried out by workers in manufacturing — a process that can be automated using assembly lines. The same is often true for digital repetitive actions as well (e.g. a "like" on Facebook). In this case the automation is often achieved by means of software known as *bots or socialbots* (when they are used on social network sites). Bots are software agents that can replace users in carrying out repetitive tasks and can easily automate several online actions. In many contexts bots are legitimate technologies as they support the user in conducting repetitive actions. For instance Wikipedia bots support the Wikipedia community in carrying out repetitive tasks to maintain the English language Wikipedia. Many bots however can be used deceptively and for illegal purposes. For instance in online games, bots can be used to cheat, causing direct damage to fair players (De Paoli & Kerr, 2010) and game businesses. Bots can also be used to "produce" reputation values on behalf of the user — by an automation of repetitive actions awarding reputation: this is, in the first place, what I call the automated production of reputation. The automated production of reputation is a form of cheating and also a deceptive use of bots that could have serious negative consequences, first of all undermining the role of trust as a social regulatory feature of interplay in the cyberworld. The goal of this paper is to explore these problems. I will do so by introducing some empirical examples, following an approach that uses empirical material to introduce what is essentially the beginning of a conceptual exploration.

In the remainder of the paper I will firstly introduce the concept of reputation and its relevance for the cyberworld. Secondly, I will substantiate the concept of the automated production of reputation and augment it with three short empirical examples (Massively Multiplayer Online Games, the social network, twitter, and the reputational hub, Klout) that justify my claims about the increasing relevance of this phenomenon. I will finally discuss the main risks that the automated production of reputation can have for the cyberworld and finally trace a perspective for further research into this subject.

Reputation in Context

At an individual level, reputation is the summary of a person's relevant past actions in the context of a specific community. It is a collective value of trust that a community awards to a person. In other words people prefer to interact with reputable persons, whose trustworthiness has been assessed by the social group to which they belong (Dasgupta, 1988). As a form of trust, reputation allows actors to reduce the complexity of action and take decisions in situations of risk when otherwise they would possess insufficient knowledge (Luhmann, 1979). As a form of trust, reputation can be seen as a functional alternative to rational prediction for the reduction of the complexity of social action. Hence, to a certain extent, reputation can be considered a form of what Taddeo (2009) calls referential trust: "the kind of trust that one develops in an unknown agent by considering only the

¹⁵ Further examples of mechanical actions awarding reputation are described in the section, Automated Production of Reputation.

recommendations about that agent provided by other agents or by other information sources, such as newspapers or television". Referential trust therefore enacts an array of expectations that people have of each other based on cross-references related to past actions. Taddeo goes on by saying that "Referential trust is one of the main kinds of trust developed in digital environments in which communication processes are easily performed". Because of this particular feature, reputation (i.e. a form of referential trust) is a concept that has been largely adopted as a way to build trust in the cyberworld (Jøsang et al. 2007).

According to Capurro (2006), in its broader sense information ethics deals with questions of digitization: the reconstruction of all possible phenomena in the world as digital information and the problems caused by their exchange, combination and utilization. This is a useful perspective for framing the phenomenon of online reputation. Indeed, we can argue that reputation in the cyberworld is a relevant example of digitization of referential trust: it is, as Dellarocas (2003) has clearly put it, a sort of digitization of the word-of-mouth existing in traditional face-to-face networks. For Dellarocas (2003, p. 1409) "Word-of-mouth networks constitute an ancient solution to a timeless problem of social organization: the elicitation of good conduct in communities of self-interested individuals who have short-term incentives to cheat one another". Even if Dellarocas adopts an atomistic and rationalistic perspective that does not capture the whole complexity of this phenomenon, he is right in saying that traditional word-of-mouth networks (what Taddeo considers trust based on communication exchanges) can be considered as an effective solution for building social order. This is possible, in particular, because word-of-mouth networks present two relevant aspects: they can support good and stable reciprocal forms of conduct among unknown participants in social interactions and they can be used for preventing deception and cheating in such interactions. These are also the issues that I consider relevant in terms of a discussion for information ethics when we have a digitization of reputation.

The creation of digitized and internet based word-of-mouth reputation networks are attempts to rebuild the key aspects of traditional networks (good conduct and cheating-prevention). Clearly, however, there are some contextual differences that must be acknowledged between traditional and digitized reputations making this a complex challenge. Indeed, it is sufficiently evident that online reputation partly differs from offline, face-to-face reputation. The problem is that, in contrast to face-to-face interactions, online interactions are dis-embedded from any specific social context (Lash, 2002). It is quite different buying a book on Amazon from a seller whose shop is in another country or instead, buying the same book from a store located in the neighbourhood where you live. In the second case you can see and touch what you are buying, you can interact directly with the seller and ask for advice. The reputation of the local seller is known in the community where you live and you can decide whether to buy also depending on the reputation awarded to the seller by the community. In the case of online interactions, many of the features of face-to-face interactions are missing. Indeed, online you are interacting with the e-commerce portal interface and not directly with the seller or the goods you are purchasing. Furthermore, you will need to place a great deal of trust in the seller and the product you are purchasing as they are described on such an interface. Online Reputation systems have been identified as a solution to bring social order and structure (Farmer & Glass, 2010) in these dis-embedded social interactions: reputation systems collect, aggregate and display ratings, votes, comments and other informational, reputational values (i.e. references) on several aspects of the online behaviour of entities (e.g. a seller, a user, a product). These reputation values are then represented¹⁶ in a variety of ways at the interface level to support online interactions (e.g. online purchases in e-commerce). Users (e.g. customers) will then base their actions (e.g. purchase from an online seller) on the values of reputation displayed on the interface (see figure 1). These informational reputations, like more traditional reputations, are also communitarian values because they are often produced by community of users (e.g. the Amazon or TripAdvisor user communities) by the mediation of reputation systems.

Because of the necessary use of informational technologies such as reputation systems in the cyberworld, the reputation of a user (or other entities) is increasingly a matter of numerical values and aggregation of these values. To capitalize on the terms used in the Call for Papers, user reputation is in many cases a matter of "bit-strings": single numerical digital values and their aggregation in meaningful numerical wholes. Indeed on many

¹⁶ See chapter 7 of Farmer and Glass, 2010 for an overview on reputation display.

web platforms user reputation is measured with points which have been awarded, the number of likes or thumbs-up received, the number of views of an informational content (e.g. a video) and so forth. Reputation systems are then systems that collect these numerical values and aggregate them into synthetic scores and finally disseminate them to other users via the interface (see figure 1). It is this process of collection, aggregation and dissemination of informational reputational items, via reputation systems and their interfaces, that is supposed to sustain users in their good conduct during their interaction with other unknown users. In the same way reputation systems are used as ways to prevent cheating by creating an informational governance mechanism based on referential and distributed trust.

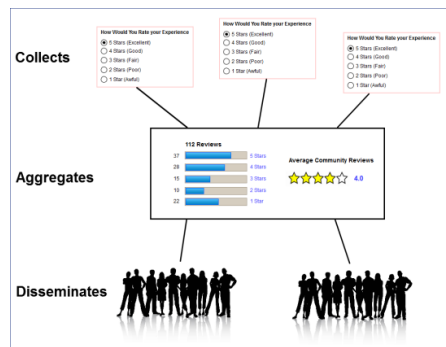


Figure 1: Concept of reputation system: collects, aggregates and disseminates reputation values

The Automated Production of Reputation

Very often, however, numerical reputation values are awarded to the user after the completion of rather mechanical and repetitive actions. As for many other contexts, repetitive and mechanical actions open the space to automation and replacement of human tasks and skills with machines¹⁷. This is clearly evident, for example, in the case of industrial labour where workers' tasks and skills are often recomposed in large industrial machineries (Marx, 1976). This is a process currently taking place also in other productive sectors, with artificial intelligence replacing skilled workers (Brynjolfsson & McAfee, 2011). What is relevant for this discussion is that the principle also works in digital contexts. In these contexts repetitive actions can be automated by means of autonomous agents, also known as bots: computer programs whose goal is to automate digital relations, replacing and supporting humans in carrying out repetitive and/or complex tasks. In many contexts, bots are legitimate technologies. For instance Wikipedia bots support the Wikipedia community in carrying out repetitive and mundane tasks to maintain the English language Wikipedia. Crawling bots, such as those used by search engines to provide users with up-to-date data about web content, are also legitimate bots. It is this consideration which opens the space for the idea of an automated production of reputation by means of machines (i.e. bots): because in many cases the actions that award reputation to a user are mechanical and repetitive and simply lead to awarding numerical values, these actions can be easily automated with bots. The automated production of reputation is then the production of reputational values with bots. The automated production of reputation is also largely a deceptive process and a violation of the shared rules of online services. Many social network sites for example explicitly forbid the use of bots and other forms of automation. This inevitably leads to a number of problems which I will discuss later in more depth. Firstly, however, it is crucial to better focus on what I mean by automated production of reputation and its deceptive nature. I will introduce three simple examples.

¹⁷ Properly what we have is a replacement of human-labour with machine labour.

Example 1: Massively Multiplayer Online Games

Firstly, I will introduce an empirical case I have studied widely over the last 3 years (De Paoli & Kerr, 2009, 2010, 2012), that of Massively Multiplayer Online Games (MMOGs) and their reputation systems: game player rankings. It was indeed the in-depth study of MMOGs that led me in the first place to observe the existence of an automated production of reputation. This example is therefore of paramount importance for building my case and I will describe it at length.

MMOGs are a sub-sector of the digital games industry (Kerr, 2007). There are hundreds of MMOGs around, with World of Warcraft often cited as the prototypical example. In MMOGs millions of players interact in a persistent Virtual World through their avatars (the in-game persona controlled by the player). A key task of MMOG game-play is that of levelling one's avatar. Avatar levelling is pursued by killing monsters inside the game: killed monsters award so called "experience points" (i.e. simple numerical reputation values) whose accumulation leads to enhancing the player's ranking inside the game. Increases in levels means that the avatar can usually perform better in the game. Rankings are an important type of reputation system in these "competitive communities" (Farmer and Glass, 2010), whose goal is to make users compete with each other¹⁸. Being at the top of the game ranking makes the user/player the most reputable in the MMOG community as this means that she has performed very well and likely better than her opponents inside the game. In this way MMOG rankings work in exactly the same manner (figure 2) as any other reputation system, as described in figure 1. Comparison between players is based on the accumulated experience points. Ranking at the top makes a player highly reputable for the MMOG community.

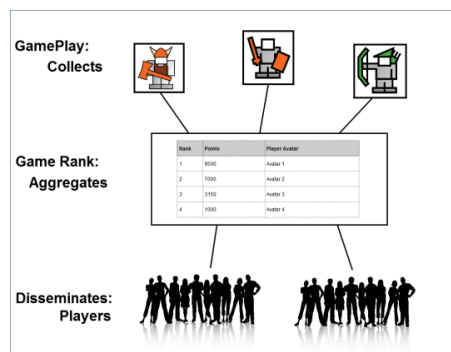


Figure 2: The concept of an MMOG rank/reputation system

Killing monsters inside an MMOG is a very repetitive and mechanical activity that requires little intellectual ability in a situation in which the player is forced to repeat the same actions over and over hundreds of times. This activity is referred to as "grinding" by players and has often been compared in academic literature to industrial labour and Taylorism (Ruggil et al, 2004). Because of this repetitiveness, many MMOGs suffer from the diffusion of bots that can replace players that can be used to automate the "grinding" MMOG levelling¹⁹. Bots can fully replace the player in killing monsters, in the subsequent accumulation of experience points and in climbing game rankings. With bots, MMOG experience points (i.e. reputation values) are clearly machine-made. This creates an unfair situation between players who play fairly (and need to manually repeat the same actions endlessly) and those who instead fully automate the levelling, since using a bot is a form of cheating. However there are further and more relevant negative consequences.

In the industrial context, automation of work is often seen as a solution to increase productivity: a reduction of the labour-time needed for producing goods. This holds true also for experience points: a direct consequence

¹⁸ Less competitive communities do not use ranks as a reputation system, as their goal is to promote collaboration rather than competition.

¹⁹ Bots in MMOGs are in any case a form of cheating and a violation of the legal documents of the games.

of automation of MMOG levelling is the increase in “productivity” as greater amounts of experience points can be easily produced in less time with bots compared to what human players can do (De Paoli, 2013). In some games, players estimate that bots can produce, in a few months, an amount of experience points that would take years for a fair player to produce (De Paoli, 2013). Bots produce more points in less time than human players (figure 3: simply provides a qualitative idea of productivity increases, it is not based on real data). This is indeed the main reason why bots are a form of cheating. In this way machine-made experience points flood the game rankings and the rankings themselves can easily become a false representation of the community reputation.

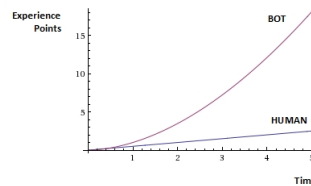


Figure 3: Machine-made versus human made experience points (time on X-Axis, accumulated points on Y-axis)

Example 2: Fake followers on twitter

Another example which displays pretty much dynamics similar to MMOGs is that of false or fake followers on twitter. Because of the wide dissemination of twitter, the phenomenon of fake followers has recently caught the attention of the media²⁰. Fake followers are machine-made followers that resemble human twitter users: they have a photo, a bio and, if well-crafted, these fake followers look like real people. In some cases they can also be backed with a bot that can entertain interactions with other users. Basically bots can fabricate these fake followers by creating real-looking twitter profiles, with the aggregation of photos and bios. Bots can produce thousands of these fake followers that can then be later sold over the internet. A twitter user can buy these followers for a few dollars and add them to her public profile (whilst violating the platform’s legal documents). As I will now show, this is a further clear example of automated production of reputation, with distinctive and deceptive outcomes.

The key aspect is that very often the number of followers that a user has on twitter is largely understood as a score or mark of the reputation and social influence of that user. The most influential people or other entities (e.g. companies) in the social media ecosystem are those that are followed by masses of followers. Justin Bieber or Lady Gaga are often quoted as examples, with the latter being the user with largest follower base (around 30 Million). Counting a single follower is again a numerical value of reputation and the total follower base can be seen as an aggregated reputation score. The equation is rather simple then, if the total number of followers — and not the quality of these followers — equals the level of reputation, then adding an increased number — if not masses — of (fake) followers can boost reputation.

As anticipated, the wide dissemination of twitter made the phenomenon of fake followers mainstream. For instance, an event that indicated the problem was the sudden increase in followers of the official twitter account of the 2012 US presidential candidate, Mitt Romney²¹, which in a span of about 24 hours had an increase of more than 100 thousand new followers (more than 10% of his total number of followers). The following graph which circulated widely in online newspapers and blogs shows some of the dynamics of this particular case

²⁰ See also a recent study by Barracuda Labs (<http://barracudalabs.com/?p=2989>) has shown the depth of this phenomenon.

²¹ This was discovered by Barracuda Labs (<http://www.barracudalabs.com/>).

and, if we focus on it, we can see that it displays pretty similar dynamics to that of figure 3²²: when automated production of reputation (machine-made fake followers added to one's account) enter the stage we have an exponential increase of values, compared to legitimate manual reputation which has a linear progression. Automated production of reputation allows an increase in productivity and floods the web with machine-made reputational values. This largely undermines the number of followers on twitter as an indicator of reputation.

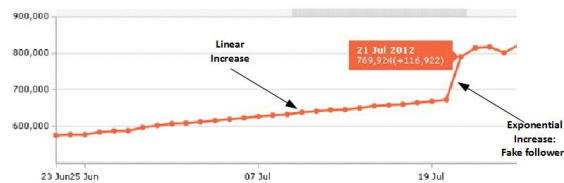


Figure 4: Fake followers and exponential increase in the Mitt Romney case²³

Recent research conducted by Camisani (2012) on Italian twitter showed that several well-known companies (both national and international companies using Italian twitter with a follower base > 10k) have in their follower base "A very high number of users with "bot" behaviour [...], with percentages in excess of 45%". The same author found that a pretty similar dynamic is displayed by the twitter accounts of Italian politicians. The author of the research concludes (in an interview) that "the number of followers is no longer a valid indicator of the popularity of a twitter user" and this, I would add, is a consequence of a larger process of automated production of reputation. In other words, the falling of the numerical model of reputation is a consequence of automation and deceptive production of reputation.

Example 3: Klout manipulation

An interesting and growing phenomenon of recent years has been the attempt to establish central reputational scores across the web, with Klout (<http://klout.com/home>) being the most successful so far. A Klout score "is a single number that represents the aggregation of multiple pieces of data about your social media activity" (<http://klout.com/corp/how-it-works>). Many signals coming from social network sites' (e.g. twitter, google+, Facebook etc.) on a user's activities are aggregated to compose the Klout score. Among them (but the list is more extensive than this), the number of likes or mentions on Facebook, the number of followers or re-tweets on twitter, the connections graph on linkedin and so forth.

An interesting post by Jeff Turner (<http://www.jeffturner.info/game-klout/>) describes an experiment that the author did to manipulate Klout largely without human intervention. By using automated software he was able to take a "Klout score of 1 to 35 in 30 days, and from 27 followers to 141". He used, in particular, a bot called replicants that is able "to simulate the activity of the user, to improve it by feeding his account and creating new contacts with other users". In this case, a Klout score has been entirely produced by bots. Turner reaches an interesting conclusion, namely, that despite prompting the idea that Klout serves as a quality indicator, in fact "Klout doesn't really care about the quality of the 'conversations' it is measuring. Klout can only care about the quantity". Reputation in centralized hubs (like Klout) that mainly leverage quantity and mechanical actions can therefore be easily produced by bots: a further clear example of the automated production of reputation. But there is more.

Having discussed the case of fake twitter followers, we can easily see a preliminary consequence: automated production of reputation in the case of fake twitter followers could also easily lead to increases (if not a major boost) in the Klout score. This is a kind of second-order effect of the automated production of reputation, which

²² Figure 3 was just a qualitative example, whereas instead Figure 4 is based on real data.

²³ Image from <http://www.nbcnews.com/technology/technolog/romney-twitter-account-gets-upsurge-fake-followers-where-928605>

does not relate just to fake followers but also re-tweets, Facebook likes and many other signals on social network sites that can be produced easily with bots. The second-order effect here is the situation in which automated production of reputation affecting a service X (e.g. twitter fake followers) also leads to increases of reputation on other services Y (e.g. boost of Klout score) that use social signals to provide reputation scores. In other words, with the central hubs that aggregate reputation values from various services, the negative consequences of the automated production of reputation could become viral for the whole social web.

Discussion: Automated Production of Reputation and its Consequences

The automated production of reputation is an emerging phenomenon touching several aspects of trust in the cyberworld. Very often this process is deceptive in nature — it is a form of cheating in social interplay and could lead to essentially negative consequences. Clearly, there are many different threats that can undermine reputation systems (Carrara & Hogben, 2007), but the automated production of reputation remains a whole new phenomenon whose direct consequences are yet to be explored.

I will now concentrate on a short focused discussion of the implications of automated production of reputation in terms of information ethics. In this regard, I second the approach of taking a critical and emancipatory perspective developing a criticism of possible consequences of the automated production of reputation in the information field, with a particular focus on the collective level. As reputation is indeed a communitarian and collective form of referential trust, this is particularly relevant. How can we then discuss the issue of the automated production of reputation in this frame? And especially its possible negative consequences on the enforcement of rules against violations and the stability of online conduct? These are relevant questions which I will now consider.

Reputation systems are practical, distributed means for internet users to support their actions and decisions. They play a relevant role in the creation of social order in the cyberworld, by engendering trust among unknown participants in online interactions of many sorts (e.g. games, commerce, plain social intercourses). They are based on what Taddeo (2009) calls referential trust: the references about an agent provided by other reliable information sources. The automated production of reputation is a problem that directly attacks this referential process by creating unreliable and fake machine-made references that could not be considered representative of an authentic collective level of trust.

Given that reputation could be easily produced by automated software, indeed a massive amount of machine-made reputation values or references could inundate the web. It takes time and effort to build a legitimate reputation. For instance, it takes quite a long time to climb the game rankings of an MMOG or to build a healthy twitter following. However, if the action that awards reputation can be replaced easily by machines and if the 'productivity' of reputation increases dramatically as a consequence, then the outcome would be that reputation (which can be considered as a form of social capital) will inevitably lose value. This is basic political economy. The value of a product is largely determined by its scarcity on the market. If scarcity is no longer an issue, then the value of the product will fall. The real problem here is for those who legitimately work hard on building their reputation (e.g. fair players, twitter users who personally manage their accounts and so forth) and then see the value of their social capital falling. This is a clear case of unfair competition and a form of cheating in social interactions.

The automated production of reputation could therefore easily lead to 'breakdowns' of reputation systems: direct consequences could be social disorder and inability to represent collective trust within active communities of users. Automated reputation-generation could, in particular, easily undermine users' ability to orient their conduct according to the level of trust being represented by reputations systems. Indeed, if the automated production of reputation becomes a mass phenomenon, then the reputation represented on reputation system interfaces will no longer be representative of the level of trust that a community has placed in a person. In other words, reputation systems will no longer be a distributed social regulatory feature of interplay upon which the user can rely when deciding with whom or what to interact in the cyberworld. This is a second and much larger negative consequence that the automated production of reputation could have on the collective level. In

brief, the automated production of reputation could easily undermine the fact that reputation in the cyberworld is meant to inherit the positive aspects of traditional Word-of-Mouth Networks (Dellarocas, 2003): stability of conduct in social interactions could fall and cheating could proliferate.

When it comes to the enforcement of rules against violations (i.e. cheating), online services have their rights as well as their responsibilities. Certainly the automatic production of reputation in most cases violates the legal documents of online services: Facebook, for instance, prohibits the use of automatic software to “like” information items, online games prohibit the use of bots to play, twitter prohibits the use of bots and the adding of fake followers and so forth. But the violation of legal documents (which I will not discuss here) is definitely not the key relevant negative consequence of automated reputation-production.

Companies (e.g. game companies, social network providers) invest heavily in information security technologies for preventing bots operating within their services or for detecting them with the goal of banning those who use bots. There are many concerns for user privacy and control over the use of these monitoring technologies. Some of these monitoring technologies act ubiquitously in the background, collecting user information and have often been criticized for being too invasive of user privacy. However, technical security solutions are not necessarily the only direction for achieving better services. The mechanical nature of reputation-generation could also be modified, and this would probably reduce the amount of privacy monitoring needed to detect bots.

Conclusion: What's next?

This manuscript is a position paper whose goal is to raise awareness of the problems emanating from the automated production of reputation and to describe some of the immediate foreseeable consequences of this phenomenon. Clearly this is not sufficient, however. Indeed, I largely believe that more needs to be done if we are to understand and tackle the problem. In this conclusion I will briefly touch upon this aspect.

In the first place, a much more solid theoretical definition of the concept of the automated production of reputation will be necessary. The description of the concept provided in this paper merely points to some possible directions of investigation, but clearly it does not have sufficient depth for theorizing about the implications that automated reputation-production has for the ‘reputation society’ at large. Possible directions for building a more solid theoretical approach have been briefly touched on in this work: the problem of productivity and the replacement of human work by technologies, the issue of the automation of work and the link with current processes of automation, the relations between reputation and the enormous internet-governance problem. Exploring these aspects more deeply, and suitably linking them with the problem of the automated production of reputation will be of paramount importance for research into reputation in the cyberworld.

Secondly, because my working approach is based on empirical research and developing theory as part of empirical data analysis (i.e. a ground-theory-driven approach), it is clear that further empirical research will be required to fully understand the boundaries, implications and evolution of the automated production of reputation. Some research fields have been described in this paper: online multiplayer games, a very dynamic and emerging field; twitter and other social network platforms as places where automated production of reputation acquires the most social form; centralized web reputational hubs that are prone to second-order negative effects depending on the automated production of reputation.

A better theory and more extended empirical fieldwork necessarily constitute the next steps in research into the automated production of reputation.

References

Brynjolfsson, E. & McAfee, A. *Race Against The Machine: How the Digital Revolution is Accelerating Innovation, Driving Productivity, and Irreversibly Transforming Employment and the Economy. [kindle edition].* Lexington MA: Digital Frontier Press, 2011.

- Camisani Calzolari, Marco. *Analysis of Twitter followers of leading international companies. Quantitative and qualitative study of behaviours demonstrated by humans (users which are presumably real) or by bots (users which are presumably fake)*, 2012. URL: <http://www.camisanicalzolari.com/MCC-Twitter-ENG.pdf>
- Capurro, Rafael, "Towards an Ontological Foundation of Information Ethics," *Ethics and Information Technology* 8, 2, (2006): 175–86 Dasgupta, Partha. *Trust as a commodity*. In D. G. Gambetta (Ed.), *Trust*: 49-72. New York: Basil Blackwell, 1998.
- Carrara, Elisabetta and Hogben Gilles. *Reputation-based Systems: A Security Analysis*. ENISA Position Paper No. 2, October 2007.
- Dellarocas, Chrysantos. *The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms*. *Management Science*, 49(10):1407-1424, 2003
- Dellarocas, Chrysantos. "Designing Reputation Systems for the Social Web". In *Building web reputation systems*, edited by Farmer, F.R. & Glass, B. 3-12. Cambridge, MA: O'Reilly, 2012.
- De Paoli, Stefano and Kerr Aphra (2009). "We Will Always Be One Step Ahead of Them": A Case Study on the Economy of Cheating in MMORPGs . *Journal of Virtual Worlds Research*, 2(4). 2009 URL: <http://journals.tdl.org/jvwr/index.php/jvwr/article/view/865/630>
- De Paoli, Stefano and Kerr Aphra. (2010). *The Assemblage of Cheating: How to Study Cheating as Imbroglia in MMORPGs*. *FibreCulture Journal*, Issue 16. 2010. URL: <http://sixteen.fibreculturejournal.org/the-assemblage-of-cheating-how-to-study-cheating-as-imbroglio-in-mmorpgs/>
- De Paoli, Stefano and Kerr Aphra. *On Crimes and Punishments in Virtual Worlds: bots, the failure of punishment and players as moral entrep*. *Ethics & Information Technology*, 14(2): 73-87, 2012.
- De Paoli, Stefano. (2013). *Bots and the Speed of Levelling: How bots change the player perception of MMORPGs*. Full paper unpublished.
- Farmer, F. Randy. and Glass, Bryce. *Building web reputation systems*. Cambridge, MA: O'Reilly, 2010.
- Jøsang, Adun, Ismail Roslan and Boyd Colin. "A survey of trust and reputation systems for online service provision." *Decision Support Systems*, vol. 43 (March 2007): 618-644, March 2007.
- Kerr, Aphra. *The Business and Culture of Digital Games: Gamework / Gameplay*. London: Sage, 2007.
- Lash, Scott. *Critique of Information*. London: Sage, 2002.
- Luhmann, Niklas. *Trust and Power*. New York: John Wiley, 1979.
- Marx, Karl. *Capital: Critique of Political Economy, Volume 1*. trans. B. Fowkes. London: Penguin, 1976.
- Masum Hassan and Tovey Mark. (eds.). *The Reputation Society: How Online Opinions are Reshaping the Offline World*. The MIT Press, 2012.
- Ruggill, Judd Ethan., McAllister, Ken S. & Menchaca, David. (2004). *The gamework*. *Communication and Critical/Cultural Studies* 1(4), 2004: 297-312.
- Taddeo, Mariarosa. *Defining Trust and E-trust: From Old Theories to New Problems*. *International Journal of Technology and Human Interaction (IJTHI)* 5(2), 2009: 23-35.

Daniel Nagel:

The Quest for a Clean Slate Building and Protecting Reputation in the Cyberworld

Abstract:

ICT technology has multiplied the possibilities for presenting who one is in the Cyberworld. The means for creating, maintaining but also of losing a good reputation have increased exponentially with an international audience now just a click away. However, these means can also be employed for abusive or, at least, purposes for which they were not intended, with undesired revelations, cyber-bullying and the creation of fake identities potentially ending in cyber-homicide. The *Quest for a Clean Slate* thus comprises multiple obstacles at various levels much like an adventure video game; no sooner are the obstacles, opponents and traps defeated or overcome and the level accomplished, than the next level begins presenting a whole host of new challenges and threats. The reputation warrior, equipped with a sword entitled "freedom to self-determination" and a humble shield entitled "legal redress", is thus thrown into the ever expanding and changing landscape of swamps and wilderness that is the Cyberworld. This paper attempts to present a sneak preview into the various levels of the *Quest for a Clean Slate*, the online reputation game, depicting its challenges, pitfalls and the possible means for overcoming these latter.

Agenda:

Introduction	24
Level 1 – You	25
Venturing out into the online world	25
The Weapons.....	25
The Main Risks.....	26
The Main Strategies.....	26
Side-stepping the Rules	27
Guerrilla Tactics	27
The Mock Battle Field	28
Know your Enemies.....	28
Level 2 – The Others	28
Venturing out into the Online World	28
The Weapons.....	28
The Main Risks.....	29
The Main Strategies.....	29
Side-stepping the Rules	30
Teaming up with other knights.....	30
Beating the enemy at their own game	30
Conclusion	30

Author:

Daniel Nagel:

- BRP Renaud & Partner, Königstraße 28, 70174 Stuttgart
- ☎ + 49 - 711 – 16445 241 , ✉ daniel.nagel@brp.de, 🌐 www.brp.de
- Relevant publications:
 - Digital Whoness: Identity Privacy and Freedom in the Cyberworld (with R. Capurro & M. Eldred) Frankfurt: Ontos Verlag 2012, 312 pp.
 - 'Beware of the Virtual Doll ISPs and the Protection of Personal Data of Minors' Nagel, Daniel Philosophy & Technology 2011 pp. 411-418 (DOI) 10.1007/s13347-011-0034

Introduction

"So it is said that if you know your enemies and you know yourself, you can win a hundred battles without a single loss. If you only know yourself, but not your opponent, you may win or you may lose. If you know neither yourself nor your enemy, you will always endanger yourself."

(Sun Tzu, The Art of War)

Presenting who we are has become increasingly more important in the advent of the cyber-age. The size of peer groups has increased exponentially and is no longer restricted to just local communities. As a result of new means of electronic communication and particularly related services such as online social networks, peer groups have started to comprise a huge variety of people pertaining to different cultural traditions irrespective of the remoteness of their actual physical location. The ubiquity of possible social interaction and the consequential increase in points of contact for new information, fresh thoughts, convictions and cultures, have heavily impacted upon digitally mediated whoness and freedom.²⁴ As whoness in turn is always a matter of having certain masks of identity reflected from the world as offers of who one could be in the world,²⁵ building reputation has become something, which is no longer solely dependent on the social acceptance of those from one's own native town. Factors such as ancestors' reputations, good looks or wealth can now be balanced or even overshadowed by reflections from the cyber-community, reflections based predominantly on how you present yourself digitally and less on other factors. However, this also means that building reputation is now having to contend with a multiplicity of new threats; ranging from negligent remarks and the publication of compromising pictures and videos resulting in defamation and slander to identity theft, indeed identity theft is said to be one of the fastest growing crimes of today.²⁶

As such, it may be said that every move we make as we attempt to navigate the glittering illusion of the online world may have a staggering impact on our reputations, having the potential to cause us considerable harm. The *Quest for a Clean Slate* is thus more than a real-life adventure game; it is, to put it more succinctly, the quest of walking the fine line between fame and shame in the Cyberworld. As with any complex adventure game, the main character in the *Quest for a Clean Slate* should be equipped with an instruction guide that outlines the various obstacles and challenges that must be overcome in order for them to master the various levels and achieve a good reputation. However, the advent of the Cyber-age has taken us by surprise; we did not have the time to adapt our education, circulate information and receive training as online warriors before being thrown into the online jungle. Our only available tactical approach has been a dangerous albeit proven method, that of trial and error, one which by its very nature involves heavy losses. The following presents a basic guide to some of the obstacles and challenges of the *Quest for a Clean Slate*. It covers two levels: level 1, which is characterised by intrinsic obstacles, including one of the biggest challenges of the Cyberworld, that of managing one's own reputation, and level 2, which is characterised by extrinsic obstacles, namely any problems posed by the outside world. This basic instruction guide also includes examples of legal remedy suggestions for both levels, discussing their respective pitfalls and benefits.

²⁴ See R. Capurro, 'Between Trust and Anxiety. On the Moods of Information Society' in *Ethical Space: The International Journal of Communication* Vol. 2, No. 4, pp. 18-21, 2004.

²⁵ See M. Eldred, in: Capurro/Eldred/Nagel: *Digital Whoness - Identity, Privacy and Freedom in the Cyberworld*, p. 28.

²⁶ See *Enhancing law enforcement and identity theft victim communications*, Identity Theft Resource Centre, fact-sheet 301, 29 August 2009.

Level 1 – You

Venturing out into the online world

"Today is the Wing Ceremony, a race to determine who graduates and becomes a knight".²⁷ One's first step into the Cyberworld is comparable to the first time a young person is invited to join a social event as a new member, thereby presenting and exposing themselves to the scrutiny of a community for the first time. However, such initiation into a political, social or religious community also traditionally incorporates safeguards; that is to say, the other members often share a common interest, follow certain standards or conventions, are prepared to welcome the invitee and sometimes already even have background knowledge about them. Despite these safeguards, it is nonetheless still possible to spoil the event and cause damage to one's reputation. In this instance, reintegration could require much effort on several subsequent occasions or the support of others, in particular senior members from the community concerned. Having said this, minor lapses are usually pardoned without much difficulty. In the Cyberworld such traditional safeguards are not however an automatic given; for example, participation in a public online discussion might concern a common issue, however, it will almost certainly attract a multitude of different stances, resulting in the level of exposure being considerably higher. In addition, whilst this community may include many benevolent participants, malicious participants can also be present. And while it is true that ICT technology may offer the possibility of concealing one's true identity, a lack of acceptance by others is still not something that can be easily shrugged off. Moreover, although using multiple online identities may help to disperse the risk of the irreversible consequences of exposure, if the objective of this level is to build one's reputation, this will also slow progress and ultimately serve to hinder the player from achieving the Holy Grail: a 'Clean Slate'.

The Weapons

The cardinal weapon is the sword of 'freedom to self-determination. Free self-determination allows the foundations to be laid for the creation of a unique identity, which, in turn, is only possible once a who finds themselves mirrored back from the world, and chooses, casts and takes on its self from this shining-back from the world.²⁸ This sword must be used to carve out decisions regarding what to reveal and what to conceal. It is a mighty weapon, which must be handled with care as it is also double-edged and while it may be used to achieve glory, it can also cause great harm both to oneself and to others.

In addition, each player is equipped with a humble shield entitled 'legal redress'. This shield may be used to fend off sword thrusts and hide the so-called privates of the player.²⁹

Finally there is a magical potion steeped in legend, the so-called 'right to be forgotten'.³⁰ Legend has it that this potion is able to cure bruises and even has the potential to heal scars. Unfortunately, as is often the case with magical potions, its recipe is hidden and heavily guarded, and no warrior has yet been able to retrieve it.

²⁷ The Legend of Zelda Skyward Sword Walkthrough and Strategy Wiki SuperGuide, 29 November 2012, at http://my-cheats.1up.com/view/section/3171340/32017/the_legend_of_zelda_skyward_sword/wii

²⁸ See J. Buchmann, (Ed.): Internet Privacy - Options for adequate realization (acatech STUDY), Heidelberg: Springer Verlag 2013 (forthcoming 2013), Chapter 1.

²⁹ Not only in the literal sense.

³⁰ See 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 (General Data Protection Regulation) COM(2012) 11 final.

The Main Risks

Level 1 of the Cyberworld is riddled with risks. While perhaps not every turn conceals a monster, it is safe to say that there is at least something hiding at every turn and about which the player must think very carefully.

The main risk of level 1 is the unwanted revelation of data. Such data might comprise a player's personal information, which could be mined, used and abused by the other players; this includes particularly personal pictures and videos. While these can be powerful tools to help improve reputation; they also carry the risk of divulging information that was intended to be kept secret. If too much information is available and falls into the wrong hands, a player's identity may also be stolen and used for other potentially malevolent purposes.

Online social networks may also pose a unique threat in and of themselves; that is to say that the risk of exposure does not only involve information that has been intentionally entered and published but also information that can be inferred from certain behaviours, connections and specifically information that has been secretly collected by the networks themselves. As such, it is not only the other players but also the networks, which must be taken into consideration when performing a thorough risk assessment. Given particularly the technical prerequisites for such networks to exist, an imbalance of power between networks and players would seem inevitable; while the network providers are armed with powerful war-horses in the form of the technical possibilities of data linkage, data mining and hidden data gathering, comparatively the players have only little ducks to come to their aid in the form of the limited privacy options granted to them. If, however, a player wishes to play the game, they must also agree to relinquish their freedom to select some of these options.

The Main Strategies

Various recommendations have been made in this respect ranging from awareness campaigns and educational approaches to technical and multidisciplinary solutions with fancy names such as 'privacy by design' or 'privacy dashboards'. While indeed simply choosing not to enter this level might be the safest way to ensure that no harm is done, it is also the surest way not to be heard. If reputation is by its very nature a reflection back from the world and the aim is to succeed in the *Quest for a Clean Slate*, becoming a recluse is simply not an option. For all those who do venture to play the game, the following details a number of potential strategies.

The most prudent strategy is to use your sword wisely, making sure to remember that it is double-edged; that is to say, it is important to fully consider the context when using your freedom to decide what to reveal and what to conceal. This context will always constitute the deciding factor when considering both levels of unwanted exposure and progress within the game.

Another strategy is to attempt to have any data that has been accidentally published, erased. Within limits, your shield can be used to do this by invoking direct and indirect rights. Note that direct rights can and must be exercised before, during and after the revelation of data:

The first step should thus always be to ensure, for example via the careful reading of terms and agreements, – even where options are limited - that levels of exposure are kept to a minimum. This involves selecting all available privacy options that do not hinder the specific aims of the player, or their agreement with other players that certain information should only be treated in a certain way.

The second step should be to closely monitor any activity whilst simultaneously protecting oneself from being blinded by the online glitter world. In this regard, the earlier a ripcord is pulled, the better. Additionally, if potential consequences are considered in due time, the risk of well-intended revelations backfiring can be considerably reduced.

The third step regards using the shield to invoke certain active rights, and is to be used if the window for the first two steps has already passed. Fundamental here, is that many legal systems recognize so-called 'personal

rights'.³¹ Depending on individual circumstances and the respective context, these rights may be used to claim the correction of certain data, the right to a counter-statement or even the right to have certain information removed. Nevertheless, the enforcement of such rights can be tricky, as the enforceability of rights is usually dependent on their political acceptance in the area concerned and the Cyberworld is not subject to clear political borders. Numerous attempts have been made to invoke specific rights in an effort shield against the risks of electronic communication,³² wherein it has been discovered that there are regulations regarding the specific areas in which these active rights may be invoked.³³

The indirect rights that may be invoked using the shield concern the obligations of the data processors.³⁴ However, these rights are less effective as they do not allow for direct enforcement. Players nonetheless have herein the option to scrutinize the acts of other players against these rules and lodge complaints if it is discovered that foul play is afoot.

In conclusion, shields must be wielded with care and utilized at the correct moment if the greatest possible protection is to be achieved, thus enabling players to proceed without too many setbacks. It must also be noted that this shield can only protect against certain elements. Players should therefore always bear in mind that the magical potion has yet to be found, and that the shield is only as good as its handler.

Side-stepping the Rules

Any regular adventure instruction guide will also include ways of side-stepping the rules; and this is no different in that it not only outlines the risks of ICT technology but also the cunning means with which to overcome them. So here are the cheats:

Guerrilla Tactics

As online social life is all about the concealing and revealing of the whoness of players in accordance with various forms of trust and security,³⁵ the guerrilla technique here is not to reveal genuine data unless it is necessary to build trust and reputation. This does not mean that blatant lying should be viewed as a helpful tool in building reputation. On the contrary, such guerrilla techniques can only be regarded as ethical if they enable the foul play of other players to be countered. Should any party request more information than is

³¹ See e.g. Article 1 and 2 of the International Covenant on Civil and Political Rights, Article II-7 et seq. Of the European Charter of Fundamental Rights, Articles 8 et seq. of the European Convention on Human Rights and Fundamental Freedoms, or as a more specific example: Article 2 in conjunction with Article 1 of the German Constitution.

³² See Resolution (73) 22 of the Council of Europe, adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies; Resolution (74) 29 of the Council of Europe Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies; The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention No. 108 dated 28 January 1981 (<http://conventions.coe.int/-treaty/en/treaties/html/108.htm>); OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data dated 23 September 1980 (http://www.oecd.org/document/18/-0,3343,en_2649_34255_1815186_1_1_1_1,00.html); Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31; Directive 2002/58/EC of the European Parliament and the Council dated 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and in particular 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 (General Data Protection Regulation) COM(2012) 11 final.

³³ See e.g. the right to information in Article 10 of Directive (EC) 95/46, the right to access in Article 12 of Directive (EC) 95/46 or the right to object in Article 14 of Directive (EC) 95/46.

³⁴ See e.g. the main principles which can be found in most of the data protection regulations, such as data minimization (See e.g. See Article 5 of the Draft Regulation COM(2012) 11 final), purpose specification (see e.g. Principle 9 of the OECD Guidelines) and the principle of consent (See e.g. Recital 33 of Directive 95/46/EC; Article 5 (3) of Directive 2002/58/EC).

³⁵ R. Capurro, Never enter your real data, IRIE Vol. 16, December 2011, pp. 74-78.

necessary or try to secretly collect data, the use of tools that prevent such acts can be a huge asset in helping players to reach the next level.³⁶

The Mock Battle Field

Another possibility is to test certain strategies within a safe environment before venturing out into the jungle. This may include testing and gathering potentially critical information via direct contact with a trusted and reliable peer group prior to starting upon level 1.

Know your Enemies

Finally, do as your enemy does, that is to say collect data on specific players. This can be a valuable activity in helping to make informed decisions regarding data reliability. As may be inferred from the Guerilla Tactics section, such data collection does not necessarily need to involve the revelation of personal data.

Level 2 – The Others

"Head for Faron Woods after stocking up on Potions and fixing your shield in Skyloft. A large boss battle is just ahead, so you'll want to be prepared."³⁷

Venturing out into the Online World

Once level 1 has been completed and the player has been dubbed a reputation knight, new dangers are to be found lurking in level 2, that of the 'other players'. The Cyberworld enables players to multiply any form of (self-) promotion and thus build reputation in a manner that up until the advent of the Cyber-age had never even been considered. The flip-side of the coin is that it is just as easy to reach such a large audience with defamatory information and so also destroy a reputation within seconds. In addition, the Cyberworld also enables new forms of attacking and seriously harming players all without the villain having to leave their cosy armchair.³⁸ As such, there is a vast multiplicity of potential attacks that other players may choose to instigate, which may be executed by a single villain or a team, subversively or openly, spontaneously or methodically and directly or indirectly, but the really frightening thing for the reputation knight is the realization that they are out there on their own or in other words: "if the victim does not do anything, no one else will".³⁹ So level 2 is all about protecting the reputation that has been built up in level 1, however, while the weapons for this level have more or less remained the same as in level 1, with only a slight upgrade, the context in which they will need to be manoeuvred has changed considerably.

The Weapons

The new sword, having been returned to the reputation knight by the blacksmith, now has the enhanced ability to slice through media and request replies.

³⁶ Such tools usually also carry fancy names such as "re-mailers", "anonymizers" or "privacy extensions".

³⁷ The Legend of Zelda Skyward Sword Walkthrough and Strategy Wiki SuperGuide, 29 November 2012, at http://my-cheats.1up.com/view/section/3171340/32017/the_legend_of_zelda_skyward_sword/wii

³⁸ Which, again, carry fancy names such as "data mining", "cyber-bullying", "trolling" or even "flame-war".

³⁹ See Enhancing law enforcement and identity theft victim communications, Identity Theft Resource Centre, fact-sheet 301, 29 August 2009.

The shield has been exchanged for one slightly larger in size and although it still does not completely cover the knight, it does now include the possibility of invoking additional rights, such as the right to claim an injunction or the right to request that the king prosecute the villains.

The magic potion, however, is still no more than a pipe dream at this stage.

The Main Risks

In level 2, the main risk faced by the reputation knight is that of being discredited by the other players. The ways in which this may occur are, however, so extensive that it would simply be impossible to even attempt to try and list them all here. Instead, two examples are considered below.

Cyber-bullying is perhaps one of the most prominent examples in this regard. Recent studies have shown that reactions to and the consequences of bullying or slander can increase exponentially if these latter are carried out in cyberspace and thus in front of a wider audience. One in ten children is estimated to be currently subject to cyber-bullying, more than half of these in a setting well-known to the knight from level 1, that of online social networks.⁴⁰ In 2010/2011, on Facebook alone, more than five million US households were said to be victims of cyber-bullying attacks.⁴¹ Reactions to the increased exposure to such attacks has similarly increased, ranging from stopping using the Internet altogether to suicides and killings prompted by cyber-bullying.⁴²

Another risk, which heavily endangers succeeding in this quest, is identity theft, a seemingly minor offence that entails severe consequences. If an identity is stolen and abused there are barely any means to make up for the damage; this is due to the fact that any act committed by the villain would seem to have been committed by the reputation knight. As such, the revelation of certain information, and any potential harm to other players would need to be rectified in order to prevent sliding down the slippery slope of public vilification.⁴³ Identity theft also entails additional pitfalls in that it is emotionally destructive and may leave the victim frightened, confused and scarred for life.⁴⁴

The Main Strategies

Creating a secure strategy to master level 2 is tricky as there are only a few preventative measures available. The best prevention is to continue to progress with care as in level 1. Both the sword and shield need to be used carefully in order to minimize making yourself a target.

If an attack is launched, the appropriate action to take will be dependent on the context, that is to say, the specific circumstances and location. The enhanced blade of the sword is unfortunately only effective if the location in which the attack occurs acknowledges the corresponding right under media law. The same applies for the new shield; while there are various means of redress both from a civil and criminal legal perspective,⁴⁵

⁴⁰ See IPSOS poll of 9 January 2012 on cyber-bullying, available at <http://www.ipsos-na.com/news-polls/pressrelease.aspx?id=5462>.

⁴¹ See Consumer Report Magazine, June 2011 available at <http://www.consumerreports.org/>.

⁴² Fortunately, the majority and especially knight minors, seem to be able to cope with cyber-bullying. See S. Livingston, L. Haddon, A. Görzig, and K Ólafsson, (2011). Risks and safety on the Internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online.

⁴³ E.g. if not, a fake profile will be created on an online social network from which fake messages attacking other players may be sent out. Many of those attacked will react with counterattacks, which will multiply the negative effects on the reputation knight.

⁴⁴ See Enhancing law enforcement and identity theft victim communications, Identity Theft Resource Centre, fact-sheet 301, 29 August 2009.

⁴⁵ From claims to erase content that is abusive to bringing criminal charges for offences.

these can – with very few exceptions -⁴⁶ only be employed on a national basis. As soon as the villain is operating from a jurisdiction where such rights cannot be enforced, the reputation knight falls into limbo. The result is comparable to a fight with the infamous and dreaded Lernaean Hydra; a victory in such a side battle would not be worth the paper it was documented on if the war were still to be lost. Nevertheless, light has appeared at the end of the tunnel with the recognition of this pitfall by the kings and their willingness to co-operate to search for a common Heracles.⁴⁷

Side-stepping the Rules

The cheats for level 2 are very similar to the ones for level 1, however, there are two additional cheats, which are worth mentioning in particular:

Teaming up with other knights

As level 2 is all about the actions of other players, this can be very helpful in countering the challenges presented in this level. The more players there are on a team, the faster they will be able to unearth, report and investigate incidents.⁴⁸

Beating the enemy at their own game

Similar to the guerrilla tactics described in level 1, there is a possibility to counter attacks using so-called technical means. This, of course, is not to be understood in the sense of 'an eye for an eye'. Rather, this aims at documenting the villain's every step, in order that they might be caught as soon as they make a wrong move, such as operating from within a jurisdiction that allows for effective prosecution.

Conclusion

Effectively building and protecting a good reputation in the online world and thereby successfully completing the *Quest for a Clean Slate* is an extremely tricky task. The weapons currently available are insufficient for the safeguarding of a fair game. Nevertheless, there is light at the end of the tunnel; considering the increasing amount of effort, which has been given to attempting to co-operate on a cross-border basis and develop new means for protecting individuals in the Cyberworld, despite the fact that the magic potion may not be discovered anytime in the near future, there is nonetheless hope that the *Quest for a Clean Slate* may be successfully completed not just as pure coincidence but as a very real and possible outcome.

⁴⁶ See e.g. Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).

⁴⁷ See the joint efforts e.g. within the United Nations Office on Drugs and Crime (<http://www.unodc.org/unodc/en/commissions/CCPCJ/institutes.html>), within Interpol (<http://www.interpol.int/>) and Europol (<https://www.europol.europa.eu/>).

⁴⁸ The most prominent example – albeit from a different level of the quest - is the use of ICT technology in Arab Springs. Another example includes associations such as the identity theft resource center (<http://www.idtheftcenter.org/>).

References

- Buchmann, Johannes (ed.): Internet Privacy - Options for adequate realization (acatech STUDY), Heidelberg: Springer Verlag 2013 (forthcoming 2013).*
- Capurro, Rafael, Eldred, Michael & Nagel, Daniel: Digital Whoness: Identity Privacy and Freedom in the Cyberworld Frankfurt: Ontos Verlag 2012,*
- Capurro, Rafael: Between Trust and Anxiety. On the Moods of Information Society, in: Ethical Space: The International Journal of Communication Vol. 2, No. 4, pp. 18-21, 2004.*
- Capurro, Rafael: Never enter your real data IRIE Vol. 16, December 2011, pp. 74-78.*
- European Commission: 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 (General Data Protection Regulation) COM(2012) 11 final*
- Identity Theft Resource Centre: Enhancing law enforcement and identity theft victim communications, fact-sheet 301, 29 August 2009.*
- Livingston, Sonia, Haddon, Leslie, Görzig, Anke, Ólafsson, Kjartan: Risks and safety on the Internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online (2011).*

Anna-Maria Piskopani:

Ethical considerations on “refreshing” digitized reputation by changing one’s name

Abstract:

In 2010 Google Chief Executive, Eric Schmidt, predicted that people will eventually be allowed to automatically change their names on reaching adulthood to escape their online past. This article attempts to follow up on such an extreme scenario in order to demonstrate the difference between erasing scattered digitized information about people’s lives and changing personal names as a method of protecting one’s reputation and identity. Such a suggested identity-erasure raises not only considerable legal and ethical considerations but also reveals an emerging stimulating debate on how the law can protect individuals from becoming their worst enemies, “haunting” them in the form of automated digitized narratives.

Agenda:

Introduction	33
Narrative identity	34
The philosophical issue	34
Digitized automated (auto)biographies	35
Protecting the self from becoming its own enemy	35
The proposal of a right to be forgotten	35
The second digitized self	36
Some ethical considerations	37

Author: Anna-Maria Piskopani

PhD candidate at the University of Athens: Piskopani Anna-Maria

- ✉ piskopania@gmail.com
- Relevant publications:
 - Piskopani Anna Maria L. Mitrou, Facebook: Reconstructing communication and deconstructing privacy law? (4th Mediterranean Conference on Information Systems. Athens 25-27 September 2009).

Introduction

In 2010, Google Chief Executive, Eric Schmidt, predicted that people will eventually be allowed to automatically change their names on reaching adulthood to escape their online past⁴⁹. In other words, he suggested that an adequate measure to protect one's reputation and informational privacy is to periodically alter one's name. Eric Schmidt referred to the example of teenagers who, while online and unaware of the possible consequences that extended exposure can have, add photos depicting themselves in intimate moments expressing extreme or controversial opinions. In their early 20s they realize the impact of such exposure to their future professional and private lives. According to Van der Hoeven's classification of harms those teenagers might experience: a) discrimination, since they can be singled out by certain social groups on the basis of misleading or incorrect assumptions based on past shared online content, b) injustice, since their personal information presented in one context can be used in a significantly different one and c) restriction of their moral autonomy, since their options for self-presentation can be limited due to the omnipresence and pervasiveness of misleading and erroneous personal information⁵⁰.

But those harms do not threaten only reckless teenagers. While in a Web 1.0 socio-environment, internet users were pursuing anonymity and using pseudonyms in the majority of their online interactions, in Web 2.0. that norm has changed. Gradually it has become more common for users participating in various social networks to use their actual names. While the rapid digitization of information in most Western societies, i.e. Big Data Practice⁵¹, has multiplied the amount of information discovered by searching one's name in a search engine, occasionally without any prior decision by the individual and without his or her awareness of those research results. The importance of erasing such information is augmenting when gossip or a false rumour is spread, when people are wrongly accused of a malicious act or crime, or are involved in an unfortunate event. So is there a new public demand to "refresh" one's digitized reputation?

Two years before the proposed EU's Data Protection Law Reform and the following debate about the implementation of a right to erase or abstain from further dissemination of erroneous or embarrassing data, the Google Chief Executive suggested another more self-regulatory path so as to resolve an increasingly troubling issue. Instead of imposing obligations on the user-generated content companies in order to minimize the negative consequences of online exposure, he has placed the burden of managing their digitized reputation on people themselves.

But what does it mean actually to change one's name? Is it just a typical bureaucratic legal procedure? Searching someone by his or her name in search engines or viewing a 6-year-old profile in social networking sites such as Facebook amounts to a chronological narration of a personal life-story. Changing one's name on reaching adulthood means beginning a brand new digital life. But the peculiar emerging situation is that the old one is not erased. The two selves coexist. A person's digital self as well as the digitized narration of their life is divided in two.

Modern philosophers such as Mac Intyre, Bruner, C. Taylor and especially P. Ricoeur, among others, have argued that not only do we exist in a story-telling world, but our very selves are constituted by the stories we and others tell about ourselves. As it has been pointed out by Ricoeur, lives like stories have a trajectory through time. What comes before affects and, to some extent, determines what follows in one's life⁵². This trajectory

⁴⁹ <http://online.wsj.com/article/SB10001424052748704901104575423294099527212.html>

⁵⁰ Information Technology, 311

⁵¹ As it has been characterized by Bert-Jaap Koops.

⁵² Oneself as another, Fifth study. Personal Identity and narrative identity.113

gives lives and stories a narrative coherence without which the story-line would give way to a mere assemblage of unrelated episodic events. Maintaining this sense of coherence is an overarching feature of a life-project and productive well-being. Narrative coherence does not concern only constructing one's identity but also one's relationship with others. It is a promise to others to behave as they anticipate based on one's emergent character and personality. In that sense a mutual trust in community is rooted in maintaining a narrative integrity. The construction of identity is closely related to a sense of responsibility towards others. Reputation is strongly related to that sense of trust between community members.

The cyberworld world is also a story-telling world. The new format of profiles in Facebook has been characterized as depicting users' life-stories, as chronological narratives⁵³. References to particular persons retrieved by searching their name appear as a credible and authoritative representation of a person's life-achievements or wrong-doings and consequently of their personal esteem, their notorious or good reputation. Is changing one's name an adequate measure to be freed from past mistakes and misfortunes? Does being narratively divided actually result in more freedom and moral autonomy, or can the construction of a double digital identity result in severe personal as well as social confusion?

In this article, we will attempt to follow such an extreme scenario in order to demonstrate the legal as well as the ethical considerations raised by such a suggestion.

Narrative identity

The philosophical issue

The discussion about whether we must have one or multiple selves recalls the philosophical debate between those who defend a notion of a disengaged self's personal identity and those who support a notion of narrative self. This debate has been analyzed by C. Taylor⁵⁴. According to Locke, and followed by Hume, the unity of the person has been disturbed because of the unusual and perplexing relation of the mind to the body. Personal identity is the identity of the self, and the self is understood as an object to be known. For Locke, personal identity is a matter of self-awareness, self-consciousness, self-perception. As Taylor points out, it was based on this philosophical tradition of a disengaged self of rational control that Parfit⁵⁵ has argued that human life is not an a priori unity or that personal identity does not have to be defined in terms of a whole life. There is only a psychological connectedness with the right kind of cause.

Both Taylor and Ricouer oppose Parfit's view. According to Taylor, referring to Heidegger's thought, the person is aware of his or her temporal dimension. Persons speak of themselves using past and future terms. So Charles points out that self-awareness has temporal depth and incorporates narrative. People are aware that they are getting older and becoming someone through maturity and regression, successes and defeats⁵⁶. In addition they make an effort for their past to be part of their life-story and to have a sense or a purpose. In other words, one's personal story must have a meaningful unity.

Simplifying this complicated debate, there are times that people look back on their past life-events and wonder whether it was really themselves who acted in a particular way. Occasionally they fail to recognize their own earlier adolescent selves and do not completely understand their motivations. But at the same time, people do

⁵³ <https://www.facebook.com/about/timeline>

⁵⁴ Sources of the self, 49

⁵⁵ Parfit Chaps. 14 and 15.

⁵⁶ Id. 50

not think that their lives started after that point so that they do recognize themselves. They are aware of their temporal continuity and realize that those past experiences made them who they are. At the same time, they are not accustomed to speaking of themselves in their early 20s by way of a third-person narrative.

Digitized automated (auto)biographies

During the last few years, people in general, and particularly young people, have been using Web 2.0 to connect and share information. They are constantly encouraged to share photos, thoughts, participation in events, feelings and life-experiences. So searching for a person by name on automated self presentational sites such as Facebook⁵⁷ can lead to a public Facebook profile. It contains personal information chronologically organized⁵⁸. Searching on other sites such as Google.com, Zoominfo.com, Pipl.com leads to a series of personal references. It is a trail of information-fragments removed from their original context.

So a person's reputation is not solely constructed by his/her interaction with others, but also by those search results. Mostly, individuals are unaware of the searches occurring as well as their results. Their digitally automated life-stories are deeply dependent on search engines' algorithms. So an internet search retells their life-stories. The individual is not the subject of this narrative, but the object. As analyzed above, this digitized, automated narrative self can harm the actual self. Recalling Ricoeur, self-constancy, objectified in the image of an interlinking of all of our acts outside of us, has the appearance of a fate that makes the self its own enemy⁵⁹. As another scholar has also noted "digital traces therefore have the potential to act as a virtual prison, to keep us tethered to expressions of ourselves that are outdated, incomplete or inaccurate"⁶⁰.

Protecting the self from becoming its own enemy

The proposal of a right to be forgotten

As analyzed above, since technology facilitates practices such as archiving information from every possible source and the construction of automated biographies, it challenges the law to protect the self from becoming its own enemy. Despite its long legal history, defamation law is limited to protecting the self only from having falsehoods spread, thus damage one's reputation, and can be implemented in few cases⁶¹. In order to resolve such problems, to respond to those personal as well as social concerns, a reform of European Union Data Protection Law has been proposed. As it has been noted that its key component is a right to be forgotten⁶². The right of individuals to have their data fully removed when they are no longer needed for the purposes for which they were collected, or when they withdraw consent, or when the storage period consented to has expired. According to the proposed reform, the obligation to erase or abstain from further dissemination of data exists if: a) they are no longer necessary in relation to the purposes for which they were collected or

⁵⁷ As is has been characterized by Werbin.

⁵⁸ At the same time it must not be neglected that those digitized automated autobiographies can have personal, economic and social value. For example, such social value is recognized in Facebook's principles. According to the 5th Principle. people should have the freedom to build trust and reputation through their identities and connections and should not have their presence on the Facebook Service removed for reasons other than those described in Facebook's Statement of Rights and Responsibilities.

⁵⁹ Oneself as another, 296.

⁶⁰ Lindsay, 422.

⁶¹ Solove 122

⁶² Mitrou/Karyda

otherwise processed, b) their processing does not comply with the data protection framework, c) the data subject withdraws her consent or objects to the processing.

The proposed reform has initiated a still vigorous debate on the nature of such rights. Many have attempted to define the right. Although some have connected to identity and have been inspired by Ricouer's thought, they do not seem to understand the importance of referring to one's self. For example, Andrade argues that a right to be forgotten broadens the scope of the right to personal identity, covering not only the entitlement to construct one's future identity-story, but also to erase one's past. He also claims that the right to be forgotten plays an essential role, not in the process of identity construction, but in the process of identity deconstruction, allowing for new and different identities to be built afterwards⁶³.

Some have wondered whether it is a right, a value or an interest. Others have examined its relationship to other rights such as self-determination, privacy, right to identity and the right to forget⁶⁴. Others have warned that legal restrictions could hinder expression and stifle freedom in the cyberworld⁶⁵. Some scholars have suggested that the right covers situations that the right to erase data already significantly protects, severely questioning whether such legal provisions can be adopted because of the digital "tsunami"⁶⁶. Most authors focus on a combination of legal and technical regulatory measures such as the implementation of PETS⁶⁷.

The second digitized self

According to the purpose of the proposed Directive Reform, individuals should require no effort or insistence to have their data deleted, as erasure should take place in an automated way. In this sense the proposed Regulation includes also a reversion of proof concerning the erasure of data⁶⁸.

On the opposite side of this proposition lies Google Chief Executive's suggestion to young people to change their names in their 20s. Such a drastic solution evokes fugitives or witnesses under police protection, the individual bearing the burden of having to conceal embarrassing personal information. Changing one's name requires substantial time and effort. While individuals' real names become a digital pseudonym leading their own separate digital lives, each leads the rest of their life with a new name, constructing a new digital self, concealing their past and in fear of it.

Apart from its not being an adequate measure to protect an individual's reputation, it must be considered that reputation is also a core component of personal identity⁶⁹. As Post has noted, reputation is the respect for the self arising from assuming full responsibility in society⁷⁰. Recalling Ricouer, these two aspects of responsibility, prospective and retrospective, join together and overlap in responsibility in the present. As he asserts, holding oneself responsible, in a manner that remains to be specified, means accepting to be held to be the same today as the person who acted yesterday and who will act tomorrow⁷¹. As recently noted, remembering is a way of ensuring the accountability of persons for the consequences of their actions, which nourishes "the sense of

⁶³ 126

⁶⁴ Andrade

⁶⁵ Rosen 88.

⁶⁶ Koops 256

⁶⁷ Mitrou/Karyda

⁶⁸ Id.

⁶⁹ Solove, 33

⁷⁰ Post 711

⁷¹ Id. 295

responsibility that is just as necessary to a democratic society"⁷². In case two or even more selves coexist, responsibility towards others is blurred. The new self is not responsible for its past actions, and the community cannot easily trust the person, since it cannot base its assessment on the individual's past actions.

Can this measure guarantee moral autonomy and freedom as it promises to do? In today's constantly connected societies, changing one's own name does not guarantee that a personal identity could be hidden. It could be easily recognized within a circle of friends and acquaintances and by via photos (facial recognition). At the same time, if changing one's name became common practice, a new kind of stigmatization might emerge. New friends and acquaintances might wonder why someone has decided to "refresh" their reputation. So it could result in discrimination and inequality. In short, changing one's name in one's 20s seem to cause more personal and social confusion than it succeeds in its purposes. This frivolous but yet distracting proposition must be totally eliminated from a nascent, fascinating discussion about the protection of the self from its digital self.

Some ethical considerations

It seems that a society that allowed young adults to easily erase their past, would neglect basic values. Young people would learn that they do not have to be taught by their past experiences. They would not need to ask for others' compassion and understanding, nor extend them to others if required. They would not deal with their own controversies nor with others. They would forget but not forgive, neither themselves nor others. They could not evaluate their own as well as others' struggle to change, to become and be taught by their own and others' narratives. It seems that such a society would accept that young people would avoid confronting basic characteristics of their own human nature: imperfection, loss and error⁷³. It would appear as a society of "flawless" people incapable of seeing one another.

References

- Allen, Anita L., Dredging Up the Past: Lifelogging, Memory and Surveillance in *University of Chicago Law Review* Vol. 75, 2008 p. 47.
- Andrade, Norberto Nuno Gomes de, 'Oblivion: The right to be different ... from oneself. Reproposing the right to be forgotten' VII International Conference on Internet, Law & Politics. Net Neutrality and other Challenges for the Future of the Internet *Idp. Revista de internet, derecho y política*. No. 13 2012, p. 122ff.
- Hoven, Jvd. Information Technology, Privacy and the Protection of Personal Data' in Weckert, J., Hoven, Jvd.; (eds.) *Information Technology and Moral Philosophy Cambridge University Press, 2008*.
- Koops, Bert.-Jaap. 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to be forgotten" in Big Data Practice 8:3 SCRIPTed Volume 8, Issue 3, December 2011, p. 229ff. Available at: <http://ssrn.com/abstract=1986719>
- Lindsay, D. The emerging right to be forgotten in data protection law: some conceptual and legal problems' in *Proceedings of the 8th International Conference on Internet, Law & Politics Challenges and Opportunities of Online Entertainment Barcelona 2012*, pp. 419 ff.
- Mitrou, M., Karyda M., 'EU's Data Protection Reform and the right to be forgotten - A legal response to a technological challenge?' *5th International Conference of Information Law, 2012, Corfu Greece June 29-30.2012*.
- Parfit, Derek *Reasons and persons Oxford University Press 1984 Chaps. 14 and 15*.

⁷² Blanchette and Johnson 2003 in Mitrou/Caryda.

⁷³ Allen

Post, Robert, 'The social foundations of defamation law. Reputation and Constitution' 74 Cal. L. Rev. 691, 1986.

Ricœur, Paul, Oneself as Another Translated K. Blamey. Chicago: U of Chicago P. 1992.

Rosen, J. 'The Right to Be Forgotten' 64 Stanford Law Review ONLINE 2012 p. 88 ff.

Solove, D. The Future of Reputation – Gossip, Rumor and Privacy on the Internet New Haven and London: Yale University Press 2007.

Taylor, Charles, Sources of the Self: The Making of Modern Identity Cambridge: Harvard U.P. 1989.

Werbin, Kerbin, 'Auto-biography: On the Immanent Commodification of Personal Information' in IRIE Vol. 17 7/2012.

Bo Zhao:

An Analytical Note: How the Internet Has Changed Our Personal Reputation

Abstract:

The internet and other new technologies have changed personal reputation fundamentally, as seen in many similar cases regarding online defamation and privacy invasion. These changes include: a) digital reputation becomes the prevailing form of personal reputation with new characteristics; b) traditional reputational networks have been updated to online networks; c) therefore the ways for individuals to establish, maintain and defend reputations are altered in the new environment; and d) many social functions traditionally played by personal reputation have been challenged by the development of digital reputation. This article tries to provide a brief analysis of such changes and sound the warning bell. We, as citizens of the new Database Nation, have to be fully aware of such changes in order to avoid potential harms while enjoying the benefits of the information age.

Agenda:

Introduction	40
Changed personal reputation	40
Reputational network updated	40
Prevailing digital reputation.....	41
New characteristics	42
Reputation management.....	43
Modified functions	44
Conclusion	45

Author:

Dr. Bo Zhao:

- Faculty of Arts and Faculty of Law, University of Groningen, the Netherlands
- ☎ + 31 - 50 - 363 9457 , ✉ B.Zhao@rug.nl
- The author is grateful to The Netherlands Organization for Scientific Research (NWO) for financial support, as well as to Jan Blaauw, Konstantin Mierau and others for helpful discussion.

Introduction

American law professor Robert Steinbuch's story shows us how the internet can damage reputation and twist life so ruthlessly.⁷⁴ Cutler, a former staff assistant working at Capitol Hill, blogged about detailed sensational sexual encounters with her colleague Steinbuch, as well as with other men she simultaneously had relations with. Her blog was connected to many social networks and soon the story got widely known both online and offline. As a promising staff attorney for Ohio Senator Mike DeWine, Steinbuch left his job for teaching. In the following years, his law students constantly kept googling his story. Embarrassed by the publicity, he lodged several legal cases against the invasion of privacy and to save his good name, but seemingly in vain.⁷⁵

In his book *The Future of Reputation*, American Law Prof. Daniel J. Solove vividly sketched what the future of our personal reputation, digitized reputation or digital reputation, could be, and how our laws should react to this depressing future.⁷⁶ Like the commercial world, the internet and new technologies have offered new ways of collecting, disseminating, processing and preserving personal information. With more than half employers use social networking sites to search job applicants,⁷⁷ we are more and more likely to be what the internet, or merely Google, says we are.⁷⁸ It is not exaggerated at all to say that the internet has made fundamental changes to our personal reputation.

An individual's reputation is a social-moral judgment of the person based on the facts considered relevant by a community; such facts include personal acts and characteristics.⁷⁹ There are various ways or instruments that individuals use to create, preserve, defend and benefit from their reputations. Personal reputation exists in complex social networks, bears some characteristics, and performs certain social functions. The large openness, easy accessibility, and unprecedented liberty of the cyberworld have made big changes to these aspects of personal reputation and therefore have brought our personal reputation to a new stage. Steinbuch's story, as well as many other similar ones, has sounded the warning bell for such big changes.

Changed personal reputation

Reputational network updated

We find individual reputations in the reputational networks of a given community.⁸⁰ These reputational networks have multiple layers. The inner layers refer to the social networks of a limited number of people. Their direct contacts and interactions lead to first-hand observations, impressions and evaluations of others. The intermediate layers include people who do not have direct contacts and interactions, but who can still wield some influences over others. These are indirect social relations such as friends' friends. Their direct contact can be easily established via existing channels to communicate trusted information. The external layers include only the audience brought by traditional mass media. In such social networks information flows only in one direction and a person has a reputation among many whom he knows nothing about. This happens to most public figures whose reputations reach beyond geographical boundaries.

⁷⁴ Known as Washingtonienne, see: Glaister, Dan: Washington Gets Ready to Gossip as DC Sex Blog Goes to Court

⁷⁵ Goldman, Eric: Robert Steinbuch Loses Another Round--Steinbuch V. Hachette

⁷⁶ Solove, Daniel J: The Future of Reputation: Gossip, Rumor, and Privacy on the Internet

⁷⁷ Guy, Social: 50% of Employers Use Social Networking Sites to Research Job Candidates

⁷⁸ Angelo, Megan: You Are What Google Says You Are

⁷⁹ McNamara, Lawrence: Reputation and Defamation: 21

⁸⁰ Craik, Kenneth H.: Reputation: a Network Interpretation

The traditional structure of reputational networks has been altered by the openness, easy accessibility and free accessibility of the internet. First of all, the internet has created virtual social networks, an independent yet no less important social sphere open to various human interactions. It is not simply the case that people just move their social networks and their daily interactions into the cyberworld. While internet users still follow the rules of conventional social networks, anonymity allows free participation and withdrawal without worrying about any negative aftermath. This likely creates public forums for free speech and free self-expression, despite potential falsity and malicious content.

The mutual support of on-and-offline social networks largely increases the use of the internet for social interactions. People may meet others first online and then start contact in real life; or *vice versa*, from online dialogue to offline group formation.⁸¹ The internet has made maintaining large social networks possible, such as college alumni networks, which are difficult to maintain by traditional communication. Online social networks also help increase life efficiency by reducing unnecessary social contacts and improving desired contacts, as evidenced by online shopping and online dating. In addition, they are a necessary tool of socialization among young generations. Nowadays a college student without Google, Facebook or twitter accounts will be a stranger to others and be left out when many social activities are organized by online social networks. Even university authorities generally feel the pressure to participate actively in online social networks for better outreach and communication with their communities.⁸²

In the past, one gained reliable information and evaluation through direct personal contact, third party talks, gossips, or mass media. Now it is still the same for many. But a new approach is found on the internet by just searching the subjects. It needs no substantive social network, and comes at almost no cost. This in a sense reduces the necessity for individuals to develop and maintain intermediate-layer social networks, although inner personal networks are still a psychological necessity. Crowd sourcing at this point is a powerful information source to meet the demands of online information enquiry.

Thus the most fundamental change is that the internet has taken place of people and mass media to be the prevailing personal information locus. In the past, when people died, their memories went with them and their reputational networks would eventually die out.⁸³ An exception is public figures or celebrities with written records, which has little to do with ordinary people. In the digital era, however, the internet can store personal information forever if such data was once "online", no matter whom the subject is. The locus of reputational networks has moved from people, traditional archives and mass media, to the internet as the best mega archive.

Finally, online reputational networks are rather reliable information sources, when compared to traditional reputational networks. Online information is not censored and selective as compared to traditional information sources. They are open to new elements, critiques and further corrections, since every web user has the potential to be a content generator. Though false information can cause temporary problems, falsity could be defeated in the long run by constant checks and scrutiny of information subjects and other web users.⁸⁴

Prevailing digital reputation

With the importance of online social networks increasing, digital reputation or digitized reputation has gradually become the prevailing form of personal reputation. This has changed our perception and practice of reputation in daily life. First, digital reputation more or less represents the social status of an individual. Someone without online information has no public identity, a clear indication of marginalized social status in general. When no proper personal information is found online, we find it hard to trust this person and make further contact with

⁸¹ Shirky, Clay: Here Comes Everybody: The Power of Organizing Without Organizations: 142–160

⁸² See e.g. Bradshaw, Karen and Saha, Souvik: Academic Administrators and the Challenge of Social-Networking Websites: 140-154

⁸³ See Craik, Reputation: 174–175

⁸⁴ Sunstein, Cass R.: Believing False Rumors: 103–105

him.⁸⁵ A proper digital identity or reputation is vital for individual success nowadays, like in the commercial world. Online rating or ranking websites, such as those ranking lawyers and university teachers, provide important information for further social interactions.

Second, the internet is not only a major information source, but also one that we trust more. Either we can find needed information on the internet unavailable from traditional sources; or we get so used to using online information so that more information is provided for awareness, comparison and correction. Now one can control the internet and censor what others say about a person. This forces reputation subjects or bearers to take their digital reputation seriously and react to untrue information. In addition, the internet never forgets. This means that a person's past can be dredged out easily for reference,⁸⁶ once such data is uploaded online. Data aggregation and computing is able to offer a more objective view of the issue of our concern. Despite false contents, most of time, one can grasp some valuable information with a bit of deliberation.

Third, in many cases, the prevailing force of digital reputation is somehow reflected in our ill judgment that is not well justified. Employers may turn down job applicants after reading a few sentences posted by their ex-lovers, or from irrelevant online bullying, even though candidates may be professionally well qualified. The reason could be that they personally just do not like the information affiliated with such applicants. The chance of such unjustified assessments has been largely increased when irrelevant information over-floods the internet.

New characteristics

As detailed above, our present individual reputations, in particular our online reputations, are more of a *panoramic* nature. They are not localized evaluations that are based on proper standards and made in suitable contexts. This first notable characteristic can be attributed to the de-contextualization and re-contextualization of online information.⁸⁷ On the one hand, reputation becomes nearer to social reality because of the availability of multiple sources and diversified judging standards. But on the other hand, the large quantity of information makes right judgment rather difficult in view of efficiency and convenience.

No one can really read all pertinent messages in their *original* contexts, when flooded with all kinds of personal data. That the internet blends the distinctions between the past and the present, and between the private and the public, has turned individual reputation into evaluation *not in a specific context* for an intended purpose, but in terms of an evaluation of all relevant information available at a particular time. This panoramic and synthesized view replaces traditional reputation that is more localized in well-defined contexts. Personal data has to be reconstructed in readers' contexts and interpreted with different meanings to guide further decisions.

A second feature is the audience friendly tendency in nowadays reputation. There are huge amount of personal data online benefiting information seekers, but in sharp contrast less restrictions on how such information should be transferred and used beyond their original purposes of collection. Moreover, data subjects have limited control over their own personal data in the new digital environments, or they even do not know the existence of such data in the wildness of the cyberworld.⁸⁸

Third, personal reputation is more propertied or commercialized in the information age. Information is currency.⁸⁹ Like privacy, reputation information evolves into a commodity for free exchange on market.⁹⁰ Celebrity

⁸⁵ Refer to Solove's personal experience. See Solove, *The Future of Reputation*: 40–42

⁸⁶ See in general, Allen, Anita L.: *Dredging up the Past: Lifelogging, Memory, and Surveillance*: 47–74

⁸⁷ Mayer-Schönberger, Viktor: *Delete: The Virtue of Forgetting in the Digital Age*: 89–90

⁸⁸ Werbin, Kenneth C.: *Auto-biography: On the Immanent Commodification of Personal Information*: 47

⁸⁹ Reading, Viviani: *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*

⁹⁰ Werbin, Kenneth C.: *Auto-biography*

status on the internet can bring economic income or other substantial benefits to reputation bearers. This encourages people to seek online attention by revealing more personal information regarding themselves and others. Lewinsky benefits from her association with Clinton even fifteen years after the affair. Cutler cashed in well her fifteen minutes' fame, but at the price of sacrificing Steinbuch's dignity.⁹¹ This tendency lies in a larger social process of the commercialization or propertization of personal information. This process started with the recognition and protection of the economic value in our likeness, names and intellectual properties.

A last characteristic is the diversified evaluation standards brought up by online social networks extending beyond geographical and chronological limits. While individual reputation is of great concern and open to public opinion, the whole world may speak on the same matter at the same time. New information will appear, together with much diversified views based on totally different morals. This will certainly change our impression, or just strengthen our old prejudices.⁹²

Reputation management

The shift of gravity of personal reputation to the digital form challenges the traditional methods of reputation management. Individuals now have new ways to establish, maintain and develop their reputations. However, when confronting challenges, they are rather vulnerable with respect to effective means of self-defence. Ordinary people can be famous online overnight expectedly or unexpectedly. The overnight celebrity, South Korean singer PSY, demonstrates the power of the cyberworld in creating a new world star. Online celebrity means popular attention, and in turn means more mouse clicks on one's names and relevant links. One can be an online celebrity because others disclosed information about him like Steinbuch. In both cases, the internet has provided a useful instrument to forge quick reputation.

Personal reputation management becomes much harder than in the pre-internet age, when cameras, smart phones and CCTVs are around us and all connected. The circulation of personal information concerning our behaviors, private or public, is hardly under control. Stepping out of our home means exactly a choice of less privacy and more exposure to the public for continuous scrutiny. The idea that a person, when walking in a crowded New York street and surrounded by many others, can still enjoy privacy, is out of date now.⁹³

Neither can one control the contents of information, nor the circulation boundary. Online defamation and cyber bullying are more popular threats to individuals, especially juveniles. Victims of online defamation and privacy invasion are in a much weaker position to defend their name due to the Streisand effect. The more one tries to correct negative information online, the more people will know about it.⁹⁴ In the wildness of the internet, law provides no sufficient remedy as witnessed in Steinbuch's situation, nor our morals. Self-defence can have certain practical uses. Some wrote to defamers and information hosts requiring the withdrawal or deletion of offensive information. Some post more information to correct the malicious contents. Others resorted to professionals such as reputationdefender who uses technical measures to push down calumnious messages of Google search results.

In this context, data holders are a vital player in online reputational games. Without their agreement and help, there is no final success against online defamation and privacy invasion. The right to be forgotten proposed by the European Commission is the first systematic legal reaction to devastating cyber-harms.⁹⁵ The proposal puts

⁹¹ Bussel, Rachel Kramer: Spanking Jessica Cutler

⁹² See in general Sunstein's discussion of group polarization. Sunstein, Cass R.: On Rumors: How Falsehoods Spread, Why We Believe Them, What Can Be Done: 32–46

⁹³ Think about the impact of Google glass in the near future.

⁹⁴ Cacciottolo, Mario: The Streisand Effect: When Censorship Backfires

⁹⁵ Reading, Viviani: The EU Data Protection Reform 2012

a legal duty on data hosts to block or remove offensive information upon the request of online defamation victims.

Modified functions

The above changes brought by the internet have modified the social functions that personal reputation performs in modern society. Reputation basically is a classification system to evaluate and separate people from each other by certain social-moral standards. For reputation subjects, reputation is self-presentation or self-promotion at public stage.⁹⁶ One performs or presents before others in order to be treated in desired ways. A university Professor can establish a reputation as a dreaded professor to gain maximum class efficiency. Reputation, as selective self-disclosure, is also an important means to control personal boundary.⁹⁷ The popular use of online social networks and online searching strengthens this role to the extent that many law professors edit their own Wikipedia pages for better public images.

Another enhanced function is the anonymous self-expression and personality construction in the cyberworld. Without reputational identification, an individual can disclose the "real self". One may post dirty words and unusual contents that he would not do in real life, trying to achieve an "ideal" reputation or identity for psychological needs. This inner-self, once identified with the external self, can cause trouble, putting the subject under social pressure for deviation from accepted social norms. Real reputation can be successfully separated from bogus reputation. But the more a person wants to benefit from online reputation, the more true information he has to reveal, the more he will be under other's scrutiny.

For reputation audience, reputation marks others' personal identity and personal boundary. At present, information from online search brings first impression of strangers, shapes our opinions of acquaintances, and even overturns our trust in close friends when unknown information is revealed. Besides, reputation nowadays puts more restrictions on a subject who claims a special identity. Thus an audience is likely to have a moral right to rely on a proclaimed reputation for further action, for example a trustable friend. Backed by crowd sourcing, the internet has considerably strengthened the power of audience in checking departed deeds. However, as above said, our judgment can be misled by the de-contextualization or re-contextualization of online information. Last, a noticeable, yet vicious use of digital reputation is to smear or defame others for various purposes like revenge or retaliation at little risk.⁹⁸

Regarding community as a whole, scholars have stressed reputation's role in providing mutual trust to reduce transaction cost.⁹⁹ Apparently this function has been developed to the best by online rating systems. However, the internet has impeded other social functions. Community as a whole, according to Post, has interest in protecting individuals' reputation to maintain civility, communal identity and social ordering.¹⁰⁰ To achieve those goals, individual reputation must be protected as an affirmation of righteous deeds that accord to certain mutually accepted moral standards to assert community's moral boundary.

The boundary breaking feature of online social networks helps break down such moral coherence, exposing previously hidden discrepancy and deviation to the public, and menacing mutual respect. This is particularly true when we regard reputation as intangible property and dignity.¹⁰¹ Similar to the cases of Cutler and PSY,

⁹⁶ Goffman, Erving: *The Presentation of Self in Everyday Life*

⁹⁷ Privacy is the contrary means in self boundary control. See: Derlega, V. J. and Chaikin, A. L.: *Privacy and Self-disclosure in Social Relationships*: 102–115

⁹⁸ Hence the proposal for criminalization of online defamation, see: Brenner, Susan W.: *Should Online Defamation Be Criminalized*

⁹⁹ See e.g., Posner, Richard: *The Right of Privacy*

¹⁰⁰ Post, R. C.: *The Social Foundations of Defamation Law: Reputation and the Constitution*

¹⁰¹ Post took reputation as honor, intangible property and dignity, but honor is less a popular concept in modern society. *Ibid.*

reputation is more of pure public attention, but less a result of hard work; and a negative reputation can be beneficial, and achieved at the price of sacrificing others' dignity.

Furthermore, present-day personal data processing has torn down the conventional separation between the public and the private spheres.¹⁰² An American website called Reportyourex offers a public forum allowing self-claimed victims to condemn ex-lovers and list their vicious deeds to warn others. But such disclosed private matters are not to be proved true.¹⁰³ Another telling example is the recently famous Duke University "Fuck List", posted by a formal female student to reveal her sensational experiences and rank her sex partners.¹⁰⁴ This is typically invasion of privacy by putting others under false light and disclosing their private lives, which will all be kept on the internet forever. As such, we are living under the heavy shadow of our past that is constructed on disclosed personal information and relative comments online. As a consequence, our personal identity development is thwarted largely when old identity sticks so closely to us.¹⁰⁵

Conclusion

In the information age, digital reputation becomes the prevailing form of reputation and online social network the unavoidable part of our social life. This has fundamentally changed our personal reputation with considerable consequences. As individuals, we have to know the pros and cons of such changes while relying more and more on online information to make decisions in social interactions. We have to know how to prevent ourselves from potential harms of online defamation and privacy invasion, while we are enjoying the numerous benefits of the information age.

References

- Allen, Anita L. 2008. "Dredging up the Past: Lifelogging, Memory, and Surveillance." *The University of Chicago Law Review* 75(1): 47–74.
- Angelo, Megan. "You Are What Google Says You Are." *Wired Business*, February 11, 2009. <http://www.wired.com/business/2009/02/you-are-what-go/>.
- Bussel, Rachel Kramer. "Spanking Jessica Cutler." *The Villagevoice*, May 31, 2006. <http://www.villagevoice.com/2005-05-31/people/spanking-jessica-cutler/>.
- Brenner, Susan W. 2007. "Should Online Defamation Be Criminalized?," *Mississippi Law Journal* 76, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=982418.
- Cacciottolo, Mario. "The Streisand Effect: When Censorship Backfires." *BBC*, June 15, 2012, sec. UK. <http://www.bbc.co.uk/news/uk-18458567>.
- Craik, Kenneth H. 2009. *Reputation: a Network Interpretation*. New York: Oxford University Press.
- Derlega, V. J., and A. L. Chaikin. 1977. "Privacy and Self-disclosure in Social Relationships." *Journal of Social Issues* 33(3): 102–115.

¹⁰² See in general Nagel's account of the public and private distinction. Nagel, Thomas: Concealment and Exposure: 17–22

¹⁰³ <http://reportyourex.com/page/10/>

¹⁰⁴ Hill, Kashmir: Will the Duke F**k List Lead to Lawsuits?

¹⁰⁵ Thus some scholars advocate online reputation bankruptcy. See e.g. Zittrain, Jonathan: The Future of the Internet--And How to Stop It: 228–229

Glaister, Dan. "Washington Gets Ready to Gossip as DC Sex Blog Goes to Court." *The Guardian*, December 28, 2006. <http://www.guardian.co.uk/technology/2006/dec/28/news.usnews>.

Goffman, Erving. 1959. *The Presentation of Self in Everyday Life*. 1st ed. Anchor.

Goldman, Eric. "Robert Steinbuch Loses Another Round--Steinbuch V. Hachette." *Blog. Technology & Marketing Law Blog*, April 14, 2009. http://blog.ericgoldman.org/archives/2009/04/robert_steinbuc.htm.

Hill, Kashmir. "Will the Duke F**k List Lead to Lawsuits?" *Above the Law*, October 4, 2010. <http://abovethelaw.com/2010/10/will-the-duke-f-list-lead-to-lawsuits/>.

Mayer-Schönberger, Viktor. 2011. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press.

McNamara, Lawrence. 2008. *Reputation and Defamation*. Oxford University Press, USA.

Nagel, Thomas. 1998. "Concealment and Exposure." *Philosophy & Public Affairs* 27(1):3-30.

Posner, R.A. 1977. "The Right of Privacy." *Ga. L. Rev.* 12: 393.

Post, R. C. 1986. "The Social Foundations of Defamation Law: Reputation and the Constitution." *Cal. L. Rev.* 74: 691.

Reading, Viviani. "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age." presented at the Innovation Conference Digital, Life, Design, Munich, January 24, 2012. <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26>.

Shirky, Clay. 2008. *Here Comes Everybody: The Power of Organizing Without Organizations*. The Penguin Press HC.

Social Guy. "50% of Employers Use Social Networking Sites to Research Job Candidates." *SociableBlog*, January 17, 2010. <http://www.sociableblog.com/2010/01/17/employers-use-social-networking-sites/>.

Solove, Daniel J. 2007. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. Yale University Press.

Sunstein, Cass R. 2010. "Believing False Rumors." In *The Offensive Internet: Speech, Privacy, and Reputation*, 91-106. Ed. Martha Craven Nussbaum and Saul Levmore. Cambridge Mass.: Harvard University Press.

———. 2009. *On Rumors: How Falsehoods Spread, Why We Believe Them, What Can Be Done*. First Edition. Farrar, Straus and Giroux.

Werbin, Kenneth C. 2012. "Auto-biography: On the Immanent Commodification of Personal Information," *IRIE International Review of Information Ethics* Vol. 17: 47-50.

Zittrain, Jonathan. 2008. *The Future of the Internet--And How to Stop It*. First Edition. Yale University Press.

Gloria Kirwan, Conor Mc Guckin:

Professional Reputation and Identity in the Online World

Abstract:

The interface between new entrants to professional disciplines, professional reputation management and social media usage is an under-researched and little understood phenomenon. A small-scale study on social media usage conducted with new social workers and teachers, working in the Irish context, revealed interesting insights into the complexities of reputation management for new professionals and the particular issues related to development of their professional reputations raised by online interactions, relationships and behaviour. Key messages for professionals and professional educators emerge from the findings outlined in this article.

Agenda:

Introduction	48
Professional Reputation	48
Methodology	48
Findings	49
Discussion	50
Conclusions	51

Authors:

Gloria Kirwan:

- School of Social Work and Social Policy, Arts Building, Trinity College Dublin, Dublin 2, Ireland.
- ☎ + 353-1-8963707, ✉ kirwangm@tcd.ie, 🌐 http://tcdlocalportal.tcd.ie/pls/public/staff.detail?p_unit=swsp&p_name=kirwangm
- Relevant publications:
 - *Social media, e-professionalism and netiquette in social work, Irish Social Worker, Autumn (2012): 9-12.*

Conor Mc Guckin

- School of Education, Trinity College Dublin, Dublin 2, Ireland.
- ☎ + 353-1-8962175, ✉ conor.mcguckin@tcd.ie, 🌐 http://tcdlocalportal.tcd.ie/pls/public/staff.detail?p_unit=education&p_name=mcguckic
- Relevant publications:
 - *Using Google Analytics to Evaluate the Impact of the CyberTraining Project., Cyberpsychology, behavior and social networking 15, No.11 (2012): 625 – 629.*

Introduction

This paper draws on data generated from a previous study in Ireland on social media usage, conducted with newly qualified teachers and social workers, which explored the issue of professional relationships and relationship boundaries in asynchronous social media environments. This article revisits the interviews from that study to mine the data to see what they reveal on the issue of professional reputation in the context of online social interactions.

Professional Reputation

In the professional context, reputation is strongly linked with the professional identity and character which new professional graduates, across various disciplines, construct for themselves and transport into their work environment. Closely associated with the concept of integrity, the foundation of a good professional reputation is built on "honesty, trustworthiness and personal character" (Cournoyer, 2008:24). Professional reputation relies on the demonstration of "high standards of professionalism" (Cournoyer, 2008:24) as well as behaviour, in general, that is consistent with responsible conduct that "adheres to social norms and values" (Eisenegger, 2009:11). As Eisenegger (2009:13) further points out, reputation is more than functional competence, it has a moral dimension. One can improve on performance of a role or a task by developing skills and knowledge, but it is difficult to recover from a moral lapse, particularly if that is associated with one's role performance. Therefore, reputation in the professional world is linked inextricably to one's perceived moral compass and anything, particularly overt behaviour on or off the job, which casts that in any doubt, may damage reputation, sometimes irreversibly. Where reputation is weak or lost, lack of public confidence in professional services can easily follow, as has been highlighted by negative public reactions to media revelations of poor performance (for discussion of the issue of confidence in a professional context see Wilson, Ruch, Lymbery and Cooper, 2011:48). Maintaining professional reputation, at an individual and profession-wide level, it seems, is a foundational cornerstone on which service delivery depends.

In the cyberworld, however, many potential pitfalls exist related to the types of information that people may share online (sometimes unwittingly). As a consequence, new professionals can quickly find their digital footprint or current online behaviour serves not to enhance but to compromise that very nascent reputation which they are seeking to establish within their chosen profession. Damage to professional reputation or engaging in behaviour (on- or off-line) which is incompatible with the newly acquired professional identity, can quickly interfere and possibly compromise the transition of a new graduate into the professional role.

Through our research on usage of asynchronous technologies, conducted with newly qualified teachers and social workers, it has been possible to gain insight into self-reported online behaviour, including the types or forms of online personae which participants adopt as well as features of their online bio-histories which participants reported on in the course of a set of focus group interviews. While the data collected over the course of the study cover a wide diversity of issues, this article focuses on what they reveal about the interface between social media relationships and professional reputation.

Methodology

Through the medium of focus group interviews (Krueger & Casey, 2009), groups of recent graduates drawn from two professions, teaching and social work, were asked to discuss the extent of their engagement (current and historical) on social media and how they experienced interaction on asynchronous media, in the post-graduation, early employment phase of their careers.

The focus group moderators facilitated discussion with the use of a pre-defined set of guide questions but also allowed free-flowing commentary into new topics throughout the interviews. The groups were recorded, transcribed and thematically analysed.

The focus group interviews scoped a wide range of issues related to social media usage among the participants. During the course of one focus group in particular, a lengthy dialogue took place between the participants on the issue of professional reputation and social media usage. The findings reported here draw heavily from the data contained within that particular focus group interview, which was conducted with a group of people who were employed as social workers in different settings and who had commenced their careers in Ireland as social workers within the last five years.

The interviews explored with participants their practices, views and experiences of asynchronous technologies (including Facebook, Blogs, Twitter, Podcasts, Wikis, YouTube and Tumblr) and how this overlaps, supports, compromises or conflicts with their newly acquired professional identity. From the collected data, information emerges regarding how the study participants conceptualised their online personae in terms of their overlap with their newly acquired professional identities. The findings discussed in this article reveal the viewpoints held by participants regarding the interaction between their online personae and the professional domain into which they are transitioning.

Findings

The focus group from which the data are drawn for this article was conducted as part of a bigger, ongoing study of recent social work and teacher graduates currently experiencing their first few years of professional employment in the Irish context. The group was mixed in terms of gender, age and ethnicity, although all participants were European in origin. All were qualified and practising social workers. The group members reported a spectrum of social media usage, ranging from a participant at one end of the spectrum who engaged in as many social media platforms as he could find to another participant who consciously avoided social media activity of any kind if possible. All participants were familiar with Facebook, LinkedIn and Twitter and because of this the discussion in general concentrated on these particular platforms, although the active social media user in the group offered additional insights into issues he had encountered on other social media sites also.

In terms of reputational issues, the group identified and discussed the public nature of social media sites, the lack of control by a person over the dissemination of information about them once it is posted, and their own observations of reputational damage related to social media usage.

In terms of the public nature of social media, the focus group participants reported personal experience of clients contacting them on Facebook or looking them up on Facebook during the active period of involvement by them as professionals with those clients. Examples were also given of Facebook friends turning up to their agency seeking a service and the potential blurring of professional boundaries this might cause. All agreed, and it had happened to one member of the group, that it would be advisable to share with their supervisor/team a situation where a Facebook friend became a client, so as to ensure that no future confusion about their management of their professional boundaries could arise. However, acknowledging the existence of an online friendship with a client, past, present or future, was only regarded as one step in a chain of decisions that flowed from such a situation. How to conduct oneself online with the client, both during and after the period of service delivery, led to debate within the group. Should online contact be suspended or terminated if a 'friend' became a client and if yes, how could that be done without causing offence or online damage to that person? Delisting a Facebook friend is a public action in an online environment, for example, and as well as causing offence it could lead to social consequences for that person.

All participants stated that they were forbidden under the terms of their employment to search online for information about their service users and any such activity on their part would therefore attract disciplinary action if they were found to have engaged in such behaviour. However, they also felt somewhat exposed to the possibility that clients could look them up online although the general consensus was that by being active

online one had to be open to this kind of scrutiny and accept that it was something over which one has no actual control.

The lack of control over the dissemination of personal information, once it is posted online, was the main deterrent for some of the participants regarding active usage of social media sites. One person had experience of information being posted in an online environment which they were unhappy about and had tried to have certain aspects of their digital bio-history removed without success. This had caused distress and had strongly influenced that person's active avoidance of online communication.

A related issue raised by participants was the online behaviour of online friends which could be viewed by others as incompatible with their own professional identity and character. Some interviewees reported that this caused them to be aware of the potential relationship between online communication and professional reputational damage. Examples were provided of group Facebook pages, for example, a class of students, where someone in the group posted offensive remarks or comments which were regarded as incompatible with responsible professional and moral behaviour. Participants (more than one) gave examples of withdrawing from such group Facebook pages when their own moral compass signalled to them that the group behaviour threatened their professional reputation. Examples of this included disrespectful comments being posted about professional colleagues or professional events.

There was also a wide-ranging discussion about the overlap between private-life activity, details of which could be posted by self or others on social media sites, and the acceptable norms of professional conduct. All participants gave examples of people they knew, that is other professionals, posting photographs, videos or written reports of activities which, in the views of the participants, fell short of accepted professional codes of conduct. The issue for the participants was the 24/7 nature of professional reputation and how reputation could quickly be lost or compromised by any behaviour (in or outside work situations) which did not conform to the ethical standards of their profession. Examples provided included online reports, sometimes contemporaneous, of social situations involving alcohol or other substances. They reported, as a particular problem, being photographed during social events and those photographs appearing online on social media pages of other people, which were then viewed by clients, employers or members of the wider profession. The invasion of social media into their private domain, whether they were active media users or not, was reported as an issue of which they were increasingly aware and which was becoming problematic for many people in their wider professional network. Again, the difficulty in erasing such digital records was a major concern to the participants and their knowledge and skill in how to manage data deletion varied considerably.

A final issue, recurring throughout the data, is the varying levels of knowledge regarding both the technological aspects of managing online communication as well as the social implications of online activity, in particular, the professional implications. During the course of the focus-group discussion, the dialogue often reverted to straightforward information-sharing about how to manage settings on different social media sites, the tracking and sharing capabilities of various technologies, and even the basics of setting up different types of accounts, construction of avatars and management of information. The issue of professional reputation in an online world saw active engagement of all of the focus group participants in the discussion but at the same time revealed varying levels of prior consideration of the topic. While some had withdrawn active engagement on particular sites out of concern that their reputation could be compromised, all were concerned that, through either their own lack of knowledge or lack of awareness or that of colleagues, their professional reputation could be easily tarnished in online environments. The message from the group for educators was that students and early stage professionals need help and guidance to work their way through the various ethical dimensions of online communication before they do something which is difficult to reverse or retrieve.

Discussion

The day-to-day management of boundary issues between professionals and their clients, be they school children or adult clients, is an issue which affects all professions. Being active on social media platforms offers a new site for social interaction with friends, family and colleagues, but it also presents new opportunities for relationship-boundary problems to arise between professionals and their client populations. For example, the

action of self-disclosure, so important for the development of online relationships (Sheldon, 2008), may present opportunities for professionals to unwittingly invade the privacy of their clients and vice versa.

The data from the focus-group interview with new social workers in Ireland revealed extensive use of asynchronous technologies by the research participants. Through the data, different perspectives emerged on the ethical component of online interaction, and its potential to interfere with, damage or possibly destroy the professional reputation which participants had worked so hard to acquire.

Although an increasing literature is emerging concerned with the ethical issues pertaining to online interaction, particularly for professionals (see for example, Teaching Council of Ireland, 2012), it appears that members of the 'always-on' generation (Belsey, 2004), fluent in their use of emerging technologies are less fluent in their awareness of the potential for online communication to interfere with their professional reputations. This may reflect the poor attention paid to online netiquette and e-professionalism across many professional education programmes (Kirwan, 2012). Research which can contribute to knowledge and education in this area, which can support the development of codes of online conduct for professionals and which can heighten awareness of the potential pitfalls, as well as the potential advantages, of online communication for professionals, is urgently necessary.

Conclusions

The data from the study of social media usage by new social workers and teachers suggest that netiquette awareness may not automatically flow from active netizenship (Bondolfi, 2013) and that professional groups themselves may need to take a leadership role in defining and supporting ethical online behaviour for individual members in much the same way as they have traditionally done in the off-line environment.

The results of this study will be of interest to professional educators but will be of particular interest to new graduates or possibly all professionals who engage in social media where they adopt a persona which may or may not be compatible with their off-line professional reputation and identity.

References

- Belsey, B: *Cyber-bullying: An emerging threat to the 'always on' generation*. 2004. Retrieved September 12, 2009, from http://www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf
- Bondolfi, T: *Netizenship*. Retrieved March 4, 2013, from: <http://www.yinternet.org/yinternet.org>
- Cournoyer, Brian R.: *The Social Work Skills Workbook*. 5th ed. Belmont, CA, Thomson Brooks/Cole. 2008
- Eisenegger, Mark: 'Trust and Reputation in the Age of Globalisation' in Joachim Klewes and Robert Wreschniok (eds.) *Reputation Capital: Building and Maintaining Trust in the 21st Century*. London, UK, Springer Verlag. 2009
- Kirwan, Gloria: *Social media, e-professionalism and netiquette in social work*. *Irish Social Worker*, Autumn (2012): 9-12.
- Krueger, R.A. and Casey, M.A.: *Focus Groups*. 4th ed. London, United Kingdom, Sage Publications. 2009.
- Sheldon, P.: *The relationship between unwillingness to communicate and students' Facebook use*. *Journal of Media Psychology* 20, (2008): 67-75.
- The Teaching Council: Code of Professional Conduct for Teachers*. 2nd ed. Maynooth, Co. Kildare, Ireland, The Teaching Council. Available at <http://www.teachingcouncil.ie/professional-standards/code-of-professional-conduct-for-teachers.1425.html>
- Wilson, Kate, Ruch, Gillian, Lymbery, Mark, and Cooper, Andrew: *Social Work. An introduction to contemporary practice*. 2nd ed. Essex, UK, Pearson Education Ltd. 2011.

Yohko Orito, Kiyoshi Murata and Yasunori Fukuta:

Do online privacy policies and seals affect corporate trustworthiness and reputation?

Abstract:

In this study, we attempt to examine the effectiveness of online privacy policies and privacy seals/security icons on corporate trustworthiness and reputation management, and to clarify how young Japanese people evaluate the trustworthiness of B to C e-business sites in terms of personal information handling. The survey results indicate that posting online privacy policies and/or privacy seals/security icons by B to C e-businesses does not work for creating trust in business organisations by consumers actively. Instead, existing good name recognition and/or general reputation can engender trust and, increasingly, better their reputation in terms of personal information use and protection.

Agenda:

Introduction.....	54
Overview of the survey	55
The survey results.....	55
Online privacy policies.....	55
Security technologies, privacy seals and security icons	58
The evaluation standards for providing personal information	58
Self-awareness and self-responsibility in terms of misuse of personal information and associated damage	60
Implications of the survey results for B to C e-business companies' trustworthiness and reputation management	61
Conclusions	62

Authors:

Dr. Yohko Orito

- Faculty of Law and Letters, Ehime University, 3 Bunkyo-cho, Matsuyama, Ehime 790-8577, Japan
- orito@ll.ehime-u.ac.jp
- Relevant publications:
 1. Adams, A. A., Murata, K., Orito, Y. and Parslow, P.: Emerging Social Norms in the UK and Japan on Privacy and Revelation in SNS, International Review of Information Ethics, 16, pp. 18-21, 2011. <http://www.i-r-i-e.net/inhalt/016/adams-etal.pdf>
 2. Orito, Y.: The Counter-Control Revolution: "Silent Control" of Individuals through Dataveillance Systems, Journal of Information, Communication and Ethics in Society, 9 (1), pp. 5-19, 2010. <http://dx.doi.org/10.1108/14779961111123197>.
 3. Adams, A. A., Murata, K. and Orito, Y.: The Japanese Sense of Information Privacy, AI & Society, 24 (4), pp. 327-341, 2009. <http://dx.doi.org/10.1007/s00146-009-0228-z>

Prof. Kiyoshi Murata

- Centre for Business Information Ethics, Meiji University, 1-1 Kanda Surugadai, Chiyoda, Tokyo 101-8301, Japan
- kmurata@kisc.meiji.ac.jp, + 81 3 3296 2165, www.kisc.meiji.ac.jp/~ethicj
- Relevant publications:
 4. Murata, K., Orito, Y. and Fukuta, Y.: Japanese Youngsters' Social Attitude towards Online Privacy, forthcoming to Journal of Law, Information and Society.
 5. Murata, K. and Orito, Y.: Rethinking the Concept of the Right to Information Privacy: A Japanese Perspective, Journal of Information, Communication and Ethics in Society, 6 (3), pp. 233-245, 2008. <http://dx.doi.org/10.1108/14779960810916237>
 6. Orito, Y. and Murata, K.: Socio-cultural Analysis of Personal Information Leakage in Japan, Journal of Information, Communication and Ethics in Society, 6 (2), pp. 161-171, 2008. <http://dx.doi.org/10.1108/14779960810888365>

Associate Prof. Yasunori Fukuta

- School of Commerce, Meiji University, 1-1 Kanda Surugadai, Chiyoda, Tokyo 101-8301, Japan
- yasuftk@kisc.meiji.ac.jp +81 3 3296 2624
- Relevant publications:
 7. Murata, K., Orito, Y. and Fukuta, Y.: Japanese Youngsters' Social Attitude towards Online Privacy, forthcoming to Journal of Law, Information and Society.
 8. Orito, Y., Kim, E., Fukuta, Y. and Murata, K.: Online Privacy and Culture: A Comparative Study between Japan and Korea, Proceedings of ETHICOMP 2011, pp. 338-346, 2011.
 9. Orito, Y., Murata, K., Fukuta, Y., McRobb, S. and Adams, A. A.: Online Privacy and Culture: Evidence from Japan, Proceedings of ETHICOMP 2008, pp. 615-622, 2008.

Introduction

Today, for general consumers living in developed countries, online shopping behaviour has become common. Given this situation, it is alleged that one of the best ways for B to C e-business organisations to preserve their high trustworthiness and good reputation regarding personal information handling and privacy protection among their customers is to post a privacy or personal information protection policy on their website to allow customers to understand how they appropriately handle personal information and address privacy issues. Another way is to put a third-party certified privacy seal and/or security icon, such as TRUSTe or BBB, on their website. In fact, a large majority of B to C e-business organisations do post their privacy or personal information protection policies and privacy seals and/or security icons on their online shopping sites.

As in other developed countries, in Japan, personal information protection by private organisations has been the subject of legislation. The Act on the Protection of Personal Information (APPI; Act No. 57 of 2003) went into effect in April 2005. Enforcement of this law has encouraged Japanese B to C e-business organisations to put their privacy or personal information protection policies, consistent with APPI, and personal information protection guidelines provided by the relevant ministries, agencies, and municipalities based on APPI, on their websites. Additionally, many Japanese business organisations have acquired the "Privacy Mark" and put it on the front page of their websites. This refers to a Japanese privacy seal scheme run by the Japan Information Processing Development Corporation (JIPDEC), an extra-governmental body of the Ministry of Economy, Trade, and Industry (METI). The Next Generation Electronic Commerce Promotion Council of Japan (ECOM: this extra-governmental body was dissolved at the end of FY 2010 and merged into JIPDEC) emphasised the importance of e-business organisations' providing a link to a well-organised and appropriately-described privacy or personal information protection policy and putting the Privacy Mark on the front page of their websites to affirm their trustworthiness and reputation to customers (ECOM, 2008).

However, there are different viewpoints on the effectiveness of online privacy policies and seals on promoting corporate trustworthiness and reputation management. For example, Pollach (2007) suggested that online privacy policies have been drafted by business organisations with the threat of privacy litigation in mind, rather than as a commitment to the appropriate handling of personal information. On the other hand, although nobody would dispute the importance of online privacy protection, many online consumers may not, in fact, read long privacy policy statements put on an online shopping site and not give much attention to a privacy seal posted on a website when they provide personal information to a site to purchase something from it. Indeed, if this is the case, do online privacy policies and seals affect consumer attitudes to corporate trustworthiness and reputation at all?

Given this background, analysing the results of questionnaire and interview surveys conducted in 2013, and taking the authors' analyses of previous surveys conducted in 2008 and 2011 (Orito et al., 2008; 2011; Murata et al., 2013) into account, this study attempts to examine the effectiveness of online privacy policies and privacy seals/security icons on corporate trustworthiness and reputation management, and to clarify how Japanese people evaluate the trustworthiness of B to C e-business sites in terms of personal information handling and any relationship between the evaluation and corporate reputation.

In light of the survey results, it appears that posting online privacy policies does not work in engendering trust among consumers. Instead, existing good name recognition and/or general reputation of the business organisation that operates a B to C e-business site can engender trust and enhance a company's reputation in terms of personal information use and protection. That is, the halo effect and the Matthew effect (Merton, 1968) can be observed with regard to corporate trustworthiness and reputation when it comes to personal information handling.

Overview of the survey

The questionnaire survey was conducted in May 2013 using the online questionnaire website. The respondents were university students at the School of Commerce of Meiji University in Tokyo, the capital city of Japan, and at the Faculty of Law and Letters of Ehime University, in the city of Matsuyama. Of the 604 survey responses (Meiji University: 340, Ehime University: 264), 600 responses were valid (336 and 264, respectively). The survey's intended population was similar to that in our questionnaire surveys conducted in 2008 and 2011. The respondents had the option of providing their real name or student number (identification number), so that follow-up interviews with students who provided their name or student number could be done. In fact, 28 respondents (Meiji University 26, Ehime University 2) were interviewed to ask follow-up questions about outcomes and to discuss certain controversial or contradictory outcomes.

Respondent attributes are shown in Table 1, and the complete questionnaire sheet is provided in the Appendix. The questionnaire's title was "Online Shopping Survey 2013", and at the start of the questionnaire it included an explicit statement — "The aim of this survey is to analyse online shopping behaviour" — to avoid priming. Tendencies of and relationships between responses to the questionnaire were examined through statistical tests, including Pearson's chi-squared test and Fisher's exact test. The proportion of respondents who had online shopping experience had increased from 71.7% in 2008 to 78.3% in 2013. Additionally, the proportion of respondents who had provided personal information to any website had increased from 83.1% in 2011 to 94.1% in 2013. Over three-quarters of those who responded in the 2013 survey had bought something online and had provided personal information to websites.

Table 1. Respondent attributes

Age	18	19	20	21	22	23+
The number of respondents (%)	183 (30.5)	82 (13.7)	163 (27.1)	104 (17.3)	45 (7.5)	23 (3.8)
Gender (%)	Male 352 (58.7)			Female 245 (40.8)		
Q5. Have you bought something on the Web? (%)	Yes 470 (78.3)			No 130 (21.7)		
Q6: Have you provided your personal information including your name, residential address, phone number and credit-card number to any website? (%)	Yes 443 (94.1)			No 28 (6.0)		

The survey results

Online privacy policies

From the survey results, more than 80% of respondents knew of the existence of online privacy policies (81.2%). This high recognition rate of online privacy policies was consistently observed in the two previous surveys, conducted in 2008 and 2011 (83.9% and 72.6%, respectively). Moreover, the proportion of respondents who considered an online privacy policy as an important element for their online shopping was 88.9%, and a similar high evaluation of the importance of online privacy policies was seen in the 2008 and 2011 surveys (74.2% and 96.8%, respectively).

On the other hand, the results of the survey conducted in 2013, as well as previous survey results, continue to indicate that more than half of the respondents who acknowledged the importance of online privacy policies when they purchased something online did not actually read the policies frequently. Table 2 shows a cross-tabulation between Q8 and Q9. As a result of a chi-squared test, it was confirmed statistically that the respondents who accepted the importance of online privacy policies for their online shopping tended to read the online privacy policies, as compared to respondents who did not regard online privacy policies as an important

element (chi-squared (1)=25.997, $p < .01$)¹⁰⁶ who seldom read them, if at all. However, more than half of the respondents who acknowledged the importance of the policies did not actually read them very frequently. Consequently, among the respondents who considered an online privacy policy to be very important or important, the proportion of respondents who answered, "I seldom read online privacy policies," was higher than the proportion of respondents who answered, "I read online privacy policies occasionally." and "I read online privacy policies frequently."

Moreover, it seems that their recognition of the importance of online privacy policies is not necessarily relevant to their practical concerns about online privacy policies. From the chi-squared test results, it was confirmed statistically that the respondents who accepted the importance of online privacy policies for their online shopping tended to worry about compliance with the policies, as compared to those who did not regard the policies as an important element (chi-squared (1)=13.456, $p < .01$)¹⁰⁷. However, this result does not mean that the many respondents who recognised the importance of the policies also paid attention to companies' compliance with them. As Table 3 shows, it is notable that more than half of these respondents answered that they rarely worried or did not worry about companies' compliance with online privacy policies. That is, even among the respondents who recognised the importance of the policies, the majority of them did not worry about whether online shopping companies actually complied with their online privacy policies.

These tendencies were the same in terms of the respondents' sense of trust in the companies' compliance with their online privacy policies. The survey results show the tendency that over three-quarters of the respondents who answered Q11 believed that companies did comply with their privacy policies (Table 4). Although the proportion of respondents who do not read online privacy policies was highest, many of them seemed to believe that many companies did comply with their online privacy policies (Table 5). Thus, regardless of their recognition of the importance of online privacy policies, or whether they had read online privacy policies, it seems that the majority of respondents believed companies did comply with online privacy policies without any reasonable ground or clear evidence for it. It is a matter of particular interest that more respondents who considered online privacy policies to be important had optimistic attitudes with regard to companies' compliance with online privacy policies.

Table 2. Important, but unread online privacy policies

		Q9 : Do you read a privacy policy when you purchase something online?				Total
		I read them frequently	I read them occasionally	I seldom read them	I have not read them at all	
Q8: Is a privacy policy an important element for your online shopping?	Very important	20	55	69	18	162
	Important	3	66	87	17	173
	Not so important	0	1	32	7	40
	Not important at all	0	0	0	2	2
Total		23	122	188	44	377

¹⁰⁶ Because of the skewed data distribution, we applied the chi-squared test to a two-by-two matrix, which consisted of two rows related to Q8 (one row includes "very important" and "important" and the other includes "not important" and "not important at all") and two columns related to Q9 (one column includes "read frequently" and "read occasionally" and the other includes "seldom read" and "never read").

¹⁰⁷ For the same reason which is described in the previous footnote, we applied the chi-squared test to a two-by-two matrix, which consisted of two rows related to Q8 (one row includes "very important" and "important" and the other includes "not important" and "not important at all") and two columns related to Q10 (one column includes "usually worry" and "sometimes worry" and the other includes "rarely worry" and "have not worried").

Table 3. Acknowledge as important but appear unconcerned about online privacy policies

		Q10: Have you worried about whether online shopping companies abide by their online privacy policies or not?				
		I usually worry about this	I sometimes worry about this	I rarely worry about this	I have not worried about this at all	Total
Q8: Is a privacy policy an important element for your online shopping?	Very important	23	77	54	8	162
	Important	7	57	97	12	173
	Not so important	0	8	29	3	40
	Not important at all	0	0	0	2	2
Total		30	142	180	25	377

Table 4. Important, and reliable company compliance with online privacy policies

		Q11. Do you believe that companies comply with their privacy policies?				
		Every company does	Many companies do	A small number of companies do	Few companies do	Total
Q8. Is a privacy policy an important element for your online shopping?	Very important	12	126	23	1	162
	Important	12	136	22	3	173
	Not so important	0	25	13	2	40
	Not important at all	1	1	0	0	2
Total		25	288	58	6	377

Table 5. Unread but reliable company compliance with online privacy policies

		Q11: Do you believe that companies comply with their privacy policies?				
		Every company does	Many companies do	A small number of companies do	Few companies do	Total
Q9: Do you read a privacy policy when you purchase something online?	I read them frequently	2	16	5	0	23
	I read them occasionally	8	99	14	1	122
	I seldom read them	12	144	28	4	188
	I have not read them at all	3	29	11	1	44
Total		25	288	58	6	377

Why do the respondents not read privacy policies but yet they believe that companies comply with online privacy policies when they shop online? To help understand this, follow-up interviews were conducted with the 28 respondents, and several common factors could be found to explain why the respondents do not read online privacy policies. Most of them mentioned that almost all online privacy policies had long statements, which were not designed to facilitate consumer understanding, and the policies were simply not easy to understand. That is, for consumers, reading an online privacy policy is bothersome. Additionally, several interviewees reported that many policies had similar content and, therefore, they were not particularly motivated to read and/or understand the policies. Some interviewees responded that it was better to have an online privacy policy, rather than no policy, and one of them said that, "If some misuse of personal information is occurring, it should be reported; if it is not happening, it is safe." Unless cases of misuse of personal information or data leakage are reported, many customers may not care about the issue. It also seems that many companies do not make active efforts to develop consumer-friendly online privacy policies.

Security technologies, privacy seals and security icons

Q23 asked respondents about their recognition of encryption technology and Q24 asked them about the meaning of the padlock icon, which is shown in the browser when they visit online shopping sites. The proportion of the respondents who understood the encryption of personal information during transmission was over half (55.9%). Conversely, the proportion of respondents who understood the meaning of the padlock icon was considerably below half (32.7%) and those who answered, "I have seen this icon, but I don't know what it represents," accounted for 50.2% of the respondents. It appears that the respondents' recognition of encryption technologies was not very high.

Additionally, many respondents did not understand the meaning of privacy seals and security icons (Table 6). The recognition of TRUSTe, Thawte, and BBB remained at a low level compared with the recognition of the Privacy Mark and VeriSign. However, the proportion of respondents who answered, "I know the meaning of the Privacy Mark," was 1.9%, and VeriSign was 1.1% in 2008, and the proportions of respondents who answered, "I have seen this icon, but I don't know what it represents," were 15.4% and 36.5%, respectively, in 2008. Thus, when mention was made of the Privacy Mark and VeriSign, the percentage of respondents who acknowledged these two seals had increased, but the majority of respondents seemed not to have a clear understanding of their meanings. When we asked one interviewee about this point, the interviewee who did not know the Privacy Mark said, "I think this is such a waste, if it requires the companies to pay the expensive cost of obtaining a Privacy Mark, because many of us don't know what it means," when this interviewee was informed of the meaning and process and cost for obtaining the Privacy Mark by one of the authors.

Table 6. Recognition of privacy seals/security icons

Do you recognise the following seal/icon? (%)	Q25:Privacy Mark	Q26:TRUSTe	Q27:Thawte	Q28:BBB	Q29:VeriSign
Yes, I know what this seal/icon represents	31 (7.1)	10 (2.3)	6 (1.4)	6 (1.4)	49 (11.2)
I have seen this seal/icon, but I don't know what it represents	93 (21.2)	31 (7.1)	39 (8.9)	42 (9.6)	159 (36.2)
I don't know this seal/icon at all	315 (71.8)	398 (90.7)	394 (89.7)	391 (89.1)	231 (52.6)

The evaluation standards for providing personal information

Q18 asks, "What characteristics does a website have to which you don't want to provide your personal information?" and Q19 asks, "What characteristics does a website have to which you feel safe to provide your personal information?" Respondents can select multiple answers to each question. The results of Q18 and Q19

are provided in Tables 7 and 8, respectively. It is easy to see that many respondents used name recognition of the websites or their operators rather than the implementation of privacy protection schemes, as a standard to evaluate the trustworthiness of B to C e-commerce sites in terms of personal information use and protection. Additionally, over half of the respondents did not want to provide information to websites that have suspect web designs and too many advertisements; such websites may have a disadvantage in some cases, even if they earnestly work to establish appropriate privacy protection schemes.

Table 7. Characteristics of websites where respondents did not want to provide personal information

Answers	Number (%)
Websites that have a low profile or are operated by low-profile companies	328 (74.0)
Websites that require too much personal information	287 (64.8)
Websites with untrustworthy reputations	272 (61.4)
Websites I do not want people to know I access	263 (59.4)
Websites that have suspect designs and too many advertisements	248 (56.0)
Websites that provide suspect goods and services	242 (54.6)
Websites that seem to fail to show well-organised privacy policies, personal information protection schemes, and security	239 (54.0)
Websites that can be accessed by the general public online	218 (49.2)
Websites that require a money transaction	99 (22.3)
Websites that provide free services	88 (19.9)
Any websites	75 (16.9)
I have no idea	5 (1.1)
Other	0 (0)

Table 8. Characteristics of websites where respondents felt safe in providing personal information

Answers	Number (%)
Websites with a high profile and high traffic, or having many users	284 (64.3)
Websites that seem to have well-organised privacy policies and personal information protection schemes	247 (55.9)
Websites that seem to maintain technological security	204 (46.2)
Websites that I and/or my friends have used	130 (29.4)
Websites whose reputation information provided by a third party is accessible	117 (26.5)
Websites that have restricted access	107 (24.2)
Online shopping websites and auction websites	91 (20.6)
Recruiting websites	88 (19.9)
Websites that allow users to communicate directly with operators of the websites	69 (15.6)
Websites operated by my acquaintances	44 (10.0)
Websites that have a preferable web design	9 (2.0)
Nothing	35 (7.9)
I have no idea	15 (3.4)
Other	0 (0)

If the most important factors for cultivating consumer trust in online businesses are name recognition and the reputation of websites and/or their operators, it would seem that the efforts of companies in terms of online privacy protection alone are not rewarded. Are there any successful measures that improve consumer recognition of company efforts on privacy protection? To examine these issues, a question that asked about the level of an online privacy policy was included in the questionnaire sheet. Q12 asked, "If you purchase products or services online that are similar in price, would you prefer to purchase them on a website that provides a highly advanced online privacy policy as opposed to a website that provides a lower level online privacy policy?" The answers are provided in Table 9. Over 90% of respondents showed positive attitudes towards a highly advanced online privacy policy.

Table 9. Differences in level of an online privacy policy

Q12: If you purchase products or services online that are similar in price, would you prefer to purchase them on a website that provides a highly advanced online privacy policy (e.g. including understandable sentences, with icons and pictures), as opposed to a website that provides a lower level online privacy policy? (%)	Yes, I 'd like to, very much	Yes, if anything	I'm not quite sure on that point	No, I would not
	188 (50.1)	154 (41.1)	30 (8.0)	3 (0.8)

In this regard, it is important to examine in detail respondents' attitudes towards online privacy protection schemes, and if they are willing to accept the development of high-level online privacy policies. Q13 was designed to investigate these points; it provided interesting results about which conditions can lead to higher interest by respondents in a company's implementation of appropriate schemes for the protection of privacy when they purchase something online (Table 10). According to the results, to some extent, respondents paid attention to the kind of personal information required from the websites; thus, the qualitative aspect of the personal information they would need to provide seems to be an important factor. Additionally, because 47.3% of respondents selected high-priced goods and services, they seem to have concerns about the protection of privacy, taking cost-benefit performance into account. Further examination is necessary to analyse these issues in this context.

Table 10. Extra attention to online privacy protection

Q13: If you purchase something online, under what circumstances is it to be noted whether the online shopping website implements a proper scheme for the protection of privacy and personal information protection?	Number (%)
Goods and services that require providing detailed personal information	178 (47.6)
High-priced goods and services	177 (47.3)
Any goods and services	115 (30.7)
Goods and services I do not want people to know I purchased	97 (25.9)
Goods and services that indicate my personal preferences	74 (19.8)
Goods and services that are indispensable in daily life	28 (7.5)
Other	0 (0)

Self-awareness and self-responsibility in terms of misuse of personal information and associated damage

Finally, we attempted to identify respondents' self-awareness of the possibility of suffering damage due to the misuse of personal information and their recognition of self-responsibility concerning such damage. Q20 asked for a general estimation of the probability of suffering some kind of damage, Q21 asked about the estimated probability of suffering damage themselves, and Q22 asked about the feeling of self-responsibility if personal information is leaked and misused by others and any damage incurred. Table 11 shows the average percentages in the responses to each question.

There was no significant difference between male and female respondents in terms of the estimated probability of their suffering some kind of damage ($t(436)=-1.943$, $p>.05$), but there was a statistically significant difference in that more female respondents reported a higher probability of self-responsibility (Q22) than male ones ($t(407.548)=-3.077$, $p<.01$). Moreover, there was a statistically significant difference in that respondents estimated a lower probability of their suffering some kind of damage versus the estimate for the public generally ($t(439)=8.548$, $p<.01$). That respondents tended to estimate a higher probability of the public's suffering damage than they would themselves, or that they believed in a higher probability of their own safety, as compared to that of the general public, is consistent with their baseless confidence in the protection of privacy for themselves, as discussed in Section 3.1.

Table 11. Self-awareness of suffering damage as a result of misuse of personal information

Questions	Average (%)
Q20: How much do you estimate the probability (%) of the public suffering some kind of damage by misuse of their personal information in the current Internet environment?	37.7
Q21: How much do you estimate the probability (%) of you suffering some kind of damage by misuse of your personal information in the current Internet environment?	31.1
Q22: If you suffer some kind of damage by misuse of your personal information as a consequence of your online shopping behaviour, to what extent are you responsible for the damage? Please estimate your responsibility as a percentage.	42.8

Implications of the survey results for B to C e-business companies' trustworthiness and reputation management

As discussed above, the survey respondents tended to recognise the importance of online privacy policies and the right to privacy, and to believe that companies complied with the online policies. However, many of them did not read online privacy policies frequently, and had optimistic expectations of companies' complying with such policies, without any clear basis for this understanding. Additionally, most of the respondents seemed not to understand the meaning of privacy seals/security icons. Thus, it cannot be said for sure that posting online privacy policies and privacy seals/security icons on online shopping websites is working to engender trust and enhance the reputation of online shopping websites in a proactive manner. Rather, the existing name reputation of online shopping websites, the general reputation of the business organisations operating online shopping websites, and ease of access to reputational information can contribute to engendering a sense of trustworthiness and a better reputation in terms of personal information use and protection.

That is, the halo effect and the Matthew effect (Merton, 1968) can be seen with regard to corporate trustworthiness and reputation for personal information handling with Japanese youngsters. If this halo effect or the Matthew effect is profound, the more business organisations with existing relatively good reputations can develop higher levels of privacy protection schemes, the more they will benefit in terms of a better reputation for privacy protection, and they will be able to collect and use more personal information from consumers. However, existing name values of websites or the businesses operating them do not guarantee that such organisations have high standards of privacy protection. If the online shopping users continue to place disproportionate weight on name reputation as an evaluation standard, it will be more difficult for them to examine the appropriateness of personal information handling by business organisations operating online shopping websites. In fact, it seems that many online shopping users have given up trying to evaluate online shopping websites by assuming that privacy protection schemes are standard in the current situation in which online privacy policies lose substantive differences and a large proportion of online consumers do not understand the meaning of privacy seals/security icons. In this regard, it is important to develop a more understandable standard to evaluate approaches to protecting the right to privacy, and to promote an understanding of the meaning of privacy seals/security icons through industry-wide efforts.

As discussed in Section 3.3, posting high-level online privacy policies or implementing user-friendly online privacy schemes can have a positive impact on the creation of consumer trust and reputation. For example, the survey conducted by Tsai et al. (2011) showed the effectiveness of an indicator that presents the level of privacy protection for the consumers' purchasing behaviours. If online privacy policies and privacy protection schemes of online shopping websites can be designed with the consumers' perspectives in mind, such websites may achieve differentiation of their approaches for privacy protection from others. For example, based on the assumption that a large proportion of consumers do not read the privacy policy thoroughly, an online shopping website that can implement practical functions in terms of privacy protection would have a competitive advantage (e.g. the development of system features that enable users to set their privacy settings in a step-wise fashion and to share such setting information with other online shopping websites). Further examination of the development of user-friendly online privacy protection schemes is necessary.

Conclusions

This study examined how Japanese youngsters evaluate the trustworthiness of B to C e-business sites in terms of personal information handling by conducting a questionnaire survey and analyses. The survey results show existing good name recognition and/or general reputation of online shopping website and their operators are a most important element in evaluating their trustworthiness, rather than posting online privacy policies and privacy seals/security icons on the websites. On the other hand, it appears that business organisations' approaches to protecting the right to privacy may possibly be recognised as an evaluation standard.

Given the Japanese situation in which the markets of B to C e-business are expanding and various kinds of goods and services are available online, it is expected that more personal information will continue to be collected, stored and utilised in business organisations operating online shopping websites. In such situations, the development of user-friendly privacy protection schemes on the basis of a proper understanding of the importance of privacy protection is essential for the growth of fair reputation management in terms of personal information protection.

Acknowledgement



The authors appreciate the really helpful suggestions for improving this paper provided by Dr Michael Eldred, the guest editor of this issue. This study was supported by the MEXT (Ministry of Education, Culture, Sports, Science and Technology, Japan) Programme for Strategic Research Bases at Private Universities (2012-16) project "Organisational Information Ethics" S1291006, the MEXT Grant-in-Aid for Scientific Research (B) 25285124, and the MEXT Research Grant-in-Aid for Young Scientists (B) 24730320.

References

- Merton, R. K. (1968): *The Matthew Effect in Science*, *Science*, 159(3810), 56-63. Available online at http://www.unc.edu/~fbaum/teaching/PLSC541_Fall06/Merton_Science_1968.pdf (accessed on 11.02.2013).
- Murata, K., Orito, Y. and Fukuta, Y. (2013): *Japanese Youngsters' Social Attitude towards Online Privacy*, forthcoming to *Journal of Law, Information and Society*.
- Next Generation Electronic Commerce Promotion Council of Japan (ECOM) (2008): *Survey on Privacy Policy and Other Similar Statements on Websites (in Japanese)*. Available online at http://www.ecom.jp/report/guideline_20080826.pdf (accessed on 20.06.2009).
- Orito, Y., Murata, K., Fukuta, Y., McRobb, S. and Adams, A. A. (2008): *Online Privacy and Culture: Evidence from Japan*, *Proceedings of ETHICOMP 2008*, 615-622.
- Orito, Y., Kim, E., Fukuta, Y. and Murata, K. (2011): *Online Privacy and Culture: A Comparative Study between Japan and Korea*, *Proceedings of ETHICOMP 2011*, 338-346.
- Pollach, I. (2007): *What's Wrong with Online Privacy Policies?* *Communications of the ACM*, 50 (9), 103-108.
- Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. (2011): *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, *Information Systems Research*, 22 (2), 254-268.

	<ul style="list-style-type: none"> 8. Websites that seem to fail to show well-organised privacy policies, personal information protection schemes, and security 9. Websites that require too much personal information 10. Websites that provide free services 11. Any website 12. I have no idea 13. Other []
<p>Q19: What characteristics does a website have to which you feel safe providing your personal information? (Multiple answers allowed)</p>	<ul style="list-style-type: none"> 1. Websites with a high profile and high traffic, or having many users (e.g. official websites, websites operated by a large organisation, and public organisations) 2. Websites whose reputation information provided by a third party is accessible 3. Websites that seem to have well-organised privacy policies and personal information protection schemes 4. Websites that seem to maintain technological security 5. Websites that I and/or my friends have used 6. Online shopping websites and auction websites 7. Websites that have restricted access (e.g. member-only websites) 8. Websites operated by my acquaintances 9. Websites that allow users to communicate directly with operators of the websites 10. Recruiting websites 11. Websites that have a preferable web design 12. Nothing 13. I have no idea 14. Other []
<p>Q20: How much do you estimate the probability (%) of the public suffering some kind of damage by misuse of their personal information in the current Internet environment?</p>	<p>[]%</p>
<p>Q21: How much do you estimate the probability (%) of you suffering some kind of damage by misuse of your personal information in the current Internet environment?</p>	<p>[]%</p>
<p>Q22: If you suffer some kind of damage by misuse of your personal information as a consequence of your online shopping behaviour, to what extent are you responsible for the damage? Please estimate your responsibility as a percentage.</p>	<p>[]%</p>
<p>Q23: Do you understand that your personal information is encrypted when you submit your personal information through an online shopping website?</p>	<ul style="list-style-type: none"> 1. Yes, I know 2. No, I don't know
<p>Q24: Do you understand the meaning of the padlock icon often shown on your browser when you visit online shopping sites?</p>	<ul style="list-style-type: none"> 1. Yes, I understand this icon 2. I have seen this icon, but I don't know what it represents 3. I don't know this icon at all
<p>Q25: Do you recognise the following seal/icon?</p>	<ul style="list-style-type: none"> 1. Yes, I know what this seal/icon represents 2. I have seen this seal/icon, but I don't know what it represents 3. I don't know this seal/icon at all
<p>Q26: Do you recognise the following seal/icon?</p>	<ul style="list-style-type: none"> 1. Yes, I know what this seal/icon represents 2. I have seen this seal/icon, but I don't know what it represents 3. I don't know this seal/icon at all
<p>Q27: Do you recognise the following seal/icon?</p>	<ul style="list-style-type: none"> 1. Yes, I know what this seal/icon represents 2. I have seen this seal/icon, but I don't know what it represents 3. I don't know this seal/icon at all



<p>Q28: Do you recognise the following seal/icon?</p> 	<ol style="list-style-type: none"> 1. Yes, I know what this seal/icon represents 2. I have seen this seal/icon, but I don't know what it represents 3. I don't know this seal/icon at all
<p>Q29: Do you recognise the following seal/icon?</p> 	<ol style="list-style-type: none"> 1. Yes, I know what this seal/icon represents 2. I have seen this seal/icon, but I don't know what it represents 3. I don't know this seal/icon at all
<p>Q30: Thank you for your cooperation with our questionnaire. If you registered your name or your student number first, and you can be available for an interview, please let us know.</p>	<ol style="list-style-type: none"> 1. Yes, I can be contacted about an interview 2. No. I can't

Ulrik Franke:

On the cyber-reputation of governments

Abstract:

Government censorship has a long history, as do attempt to motivate it. This paper offers an analysis of the proposal that states should agree to cooperate "in curbing the dissemination of information that [...] undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment". This position was adopted in 2011 by the People's Republic of China, Russia, Tajikistan, and Uzbekistan in a proposed *International code of conduct for information security*. The code of conduct can be understood as an attempt to protect the cyber-reputations of states and incumbent governments from the impact of compromising information. The article examines the code of conduct from the perspectives of utilitarianism and moral rights theories. Despite some interesting minor exceptions, it is concluded that neither normative theory can fully endorse the proposed code of conduct.

Agenda:

Introduction	67
The code of conduct	67
Utilitarianism	68
Act utilitarianism	68
Rule utilitarianism.....	68
Rights-based theories	69
Conclusion	70

Author:

Dr. Ulrik Franke:

- Swedish Defence Research Agency (FOI), SE-164 90 Stockholm, Sweden
- ☎ + 46 - 8 – 5550 3504 , ✉ ulrik.franke@foi.se, 🌐 www.foi.se

Introduction

Governments have long attempted to censor and curb unwanted information, but the advent of modern information and communication technology (ICT) has changed the playing field. Today, the amount of information available is larger, it spreads quicker, and physical distance matters less. The Wikileaks controversy and the role of ICT in the Arab spring are just a few examples of recent events that have caused a lot of debate.

This paper offers an analysis of the proposal that states should agree to cooperate "in curbing the dissemination of information that [...] undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment". This position was adopted in 2011 by the People's Republic of China, Russia, Tajikistan, and Uzbekistan in a letter to the United Nations secretary general, proposing an "International code of conduct for information security" (Li et al., 2011).

The code of conduct can be understood as an attempt to protect the *cyber-reputations of states and incumbent governments* from the impact of compromising information. Political, economic and social stability is proposed as the good underpinning these restrictions on free speech online. This article examines this proposal from two normative perspectives: utilitarianism and moral rights theory.

How could such damaging information look in practice? Many scenarios are possible, but the recent case of Vladimir Pekhtin is poignant. Pekhtin was a member of the Russian Duma, chairing its Ethics committee. In February 2013, he resigned his position after opposition bloggers had made documents available that exposed his \$1.3 million real estate in Florida. The documents were not leaked, but publicly available on the Miami-Dade County government website. In a final address, Pekhtin remarked that "our opponents [...] need to discredit the Parliament, the authorities, which are represented by every person sitting in this hall, and every one of us may turn out to be a target for them" (Barry, 2013).

The article unfolds by first briefly reviewing the code of conduct itself, then analysing it from the perspectives of utilitarianism and rights-based theories, respectively. The article ends with a few concluding remarks.

The code of conduct

The proposed *International code of conduct for information security* was submitted as an annex to a letter from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. It has the form of a potential General Assembly resolution. The purpose is said to be "to identify the rights and responsibilities of States in information space [...] so as to ensure that information and communications technologies, including networks, are to be solely used to benefit social and economic development and people's well-being" (Li et al., 2011).

Following a pre-ambule, the actual code of conduct is composed of 11 articles (a-k), where the main thrust is in article b, where the signatories pledge "Not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies".

However, the focus of this article is rather article c, the pledge "To cooperate in combating criminal and terrorist activities that use information and communications technologies, including networks, and in curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment".

If the code is ever signed into effect, it is not clear whether the signatories would comply with it. There is a large body of literature suggesting that democracies are more likely to comply with international agreements than are authoritarian regimes (cf. Simmons 1998 for a review). Given that all four originators are deemed "not free" by Freedom House (2013), the initiative might be an attempt to limit the freedom of action for others

(democracies) but retain it for oneself. At least one analysis claims that this is the ulterior motive behind Russian initiatives in the field of "international information security" (Giles, 2011). While noting these concerns, this article does not take a stand on any hidden agendas or motives. Rather, the analysis proceeds by taking the proposal at face value, aiming to judge it fairly from the perspectives of the normative theories chosen. A more elaborate analysis of the code of conduct in the context of diplomatic initiatives related to so called cyber-warfare is given by Meyer (2012).

Utilitarianism

From any utilitarian perspective, the code of conduct is strangely *asymmetric*. Utilitarianism not only requires that information with *bad* consequences is *not* disseminated, but also that information with *good* consequences *is* disseminated. Thus, the preference for status quo (i.e. not undermining stability) is not a priori endorsed by utilitarianism. Rather, the utility of the status quo and the utility of any alternative state of affairs are to be assessed by the same normative standards, though there might be epistemic differences in their ease of evaluation. The analysis now unfolds by considering *act* and *rule* utilitarianism separately. This distinction is elaborated in many introductory textbooks on ethics, for example Tännsjö (2002).

Act utilitarianism

Act utilitarianism does not endorse signing *and complying* with any codes of conduct. Regardless of earlier agreements, the utilities of the alternatives at hand always remain the singular moral decision-criterion for the act utilitarian. In this spirit, however, act utilitarianism might endorse signing a code of conduct *without* (necessarily) complying afterwards. Instead the utility of the act would be brought about by affecting the future acts of others (since by hypothesis, future acts of the signatory itself are not affected). The analysis of signals and the effects on acts of others brings us very close to *rule utilitarianism*, which we will now analyze as the more plausible utilitarian candidate to warrant the code of conduct. The act utilitarian loophole of signing but not adhering will then be revisited.

Rule utilitarianism

The possible utility of upholding state reputations is two-fold: (i) *Symbolic* utility bestowed intrinsically by reputation, e.g. citizens' utility of being proud of their government. (ii) Utility where reputation is *instrumental* to another good, e.g. citizens' pride in their country driving work to improve the functioning of political, economic and social systems – or citizens' pride in their country preventing revolutionary violence. The rule utilitarian, making rules for disseminating information, has to maximize the sum of both utilities.

Recent research on the subjective appreciation of poetry might help with the empirics of symbolic utility: individuals experience greater utility when reading a poem, if convinced that it was written by a highly regarded poet (Bar-Hillel et al., 2012). If the same is true for the aesthetic appreciation of flag waving and national anthems (live or on YouTube), then that is a utilitarian argument for curbing information that discredits states: individuals might experience greater utility if convinced that they live in the best of states, than if informed (or misled) to believe that they do not.

Nevertheless, instrumental utility is probably more important (in the sense that food, housing, health etc. are probably more important than the aesthetic appreciation of poetry – at least this holds psychologically true in many circumstances, cf. Maslow 1943). On the *negative* side, revolutionary upheavals are the greatest threat (and the chief concern of China et al.). The danger of pointless revolutionary violence was famously discussed by Burke, and made Hobbes embrace the absolute power of the sovereign. This is perhaps the strongest utilitarian reason for protecting the reputations of incumbent regimes. However, even if the consequences of revolutions are dire, it does not necessarily follow that the reputations of status quo should be preserved at all

costs. As argued by Taleb & Blyth (2011) in the wake of the Arab spring, artificial suppression of volatility might merely postpone the inevitable:

“Such environments eventually experience massive blowups, catching everyone off-guard and undoing years of stability or, in some cases, ending up far worse than they were in their initial volatile state. Indeed, the longer it takes for the blowup to occur, the worse the resulting harm in both economic and political systems.”

This line of reasoning naturally leads to the *positive* side of variable reputations: they can serve as an error-correcting and efficiency-improving mechanism. Reputation systems on e-commerce websites enable sellers of high-quality goods to receive decent payments, while preventing fraudsters or sellers of low-quality goods from profiteering on unsuspecting buyers (Resnick et al., 2000), defying Akerlof’s infamous “market for lemons” (Akerlof, 1970). But such systems cannot work if reputations cannot be ruined. While incumbent governments are not E-bay peddlers, ICT-fostered transparency can plausibly reduce corruption (Bertot et al., 2010). If the reputation of an incumbent regime is allowed to deteriorate when that regime performs poorly, that can help avoid the brittle and dangerous state of affairs that so worries Taleb & Blyth. If seen from this perspective, it might be telling that the governments of China, ranked 80 in the Transparency International *Corruption Perceptions Index 2012*, Russia, ranked 133, Tajikistan, ranked 157, and Uzbekistan, ranked 170 (Transparency International, 2012), endorse a code of conduct that fosters less transparency.

Interestingly, recent political psychology research finds that the two categories of symbolic and instrumental utility are *psychologically* separate: “Exploratory factor analyses of the symbolic and instrumental items yielded two distinct and virtually orthogonal factors” (Schatz & Lavine, 2007). This means that information that decreases symbolic utility (e.g. by questioning and re-evaluating national myths, historical “truths” or great leaders) does not necessarily decrease the instrumental utility (e.g. the propensity of public sector clerks to fulfill their duties or of people to obey laws). However, some kinds of information that decreases symbolic utility (e.g. exposing corruption or identifying kleptocratic rulers) is a prerequisite for some increases in instrumental value (e.g. getting rid of corruption or ousting unfit office-holders). This is consistent with the observation of Ahlerup & Hansson (2011), who find that from an economic perspective (bearing in mind the importance placed on economic welfare by utilitarianism) the level of nationalism is higher than optimal in most countries, diminishing government effectiveness.

The position of rule utilitarianism can now be properly evaluated. Rule utilitarianism differs from act utilitarianism by considering not only the immediate, static, consequences of acts, but instead emphasizes incentives and dynamic consequences. Seen from this perspective, it seems that although agreements that protect the reputations of incumbent governments might avoid some short term damage (viz. revolutionary upheavals), this gain is far from certain, whereas the losses in the long run (viz. the incentives for corruption and kleptocracy) are virtually unavoidable. Rule utilitarians should select the dynamic error correction-mechanism of reputations that reflect merits, rather than the static status quo-preserving code of conduct. This conclusion becomes even more plausible since the instrumental utility is psychologically independent from the symbolic utility – the gains of error-corrections are to be had without loss of appreciation for flags and anthems.

Having examined some plausible consequences of the code of conduct, we can now return to the act utilitarian possibility of signing but not adhering. Following the analysis above, there is no indication that the utility of sign-not-comply would be greater than the (rule utilitarian) sign-and-comply, which on a balance is unlikely to be endorsed by rule utilitarianism. Thus, act utilitarianism as a foundation for the code of conduct can be ruled out on the same grounds.

Rights-based theories

Moral rights theory ascribes rights to individuals rather than incumbent governments, and does not care for political, economic or social stability – “liberty upsets patterns”, as put by Nozick (1974). Thus, *prima facie*, it offers scarce support for protecting the reputations of states. On the contrary, the property rights of individual

Internet users, content providers such as Facebook or YouTube, and Internet service providers protect dissemination of information from state interference. This protection of free speech echoes the *Reporters without borders* condemnation of the code of conduct as "a concept that in reality is aimed as [sic!] legitimizing censorship" (Reporters without borders, 2012). Ultimately, the right to self-ownership allows everyone to maintain whatever perception they like about others, including states, and attempts to protect one's reputation must be non-coercive.

However, rights-based theories offer two interesting cases where the dissemination of information may be curbed. First, under a theory of *positive rights*, governments may legitimately provide basic ICT services to citizens, collapsing the distinction between state and service provider. Then, service provider property rights offer no protection against state interference. Second, the emphasis placed by rights-based theories on *voluntary contracts* opens a legitimate possibility for curbing any information dissemination that breaches terms of service. For example, the use of fake personas on social networks to influence opinions – so called *sock-puppetry* – typically constitutes such a breach. Programs for this kind of influence operations have been recently exposed both in the US (Fielding and Cobain, 2011) and in Russia (Barabanov et al. 2012). Such breaches of contract constitute rights violations, and rights-based theories sanction that the offended service provider ceases service and uses government institutions, e.g. police, to seek restitution. However, the wording in the code of conduct clearly warrants much more information curbing than can be plausibly claimed legitimate under the terms of service interpretation of rights-based theories. Thus, the code of conduct as a whole cannot reasonably be endorsed by moral rights theory.

Conclusion

Article b in the proposed *International code of conduct for information security* deals, in a sense, with the cyber reputations of states, or at least their incumbent governments. It makes a normative claim that political, economic and social stability are goods that warrant certain restrictions on free speech online; limiting what kind of information may be spread. States, it argues, ought to co-operate in curbing the dissemination of such harmful information.

Having examined these claims from the perspectives of utilitarianism and moral rights theories, it is concluded that neither normative theory can fully endorse the code of conduct. Though there are conceivable cases when states would be warranted to co-operate in curbing some information harmful to their reputations, these cases are clearly the exception, not the rule. This conclusion gains additional force from the fact that it is broadly supported by two normative theories oftentimes opposed to each other.

References

- George A. Akerlof: *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, *The Quarterly Journal of Economics*, Vol. 84, No. 3, August, 1970, pp. 488-500
- Pelle Ahlerup & Gustav Hansson: *Nationalism and government effectiveness*, *Journal of Comparative Economics*, Vol. 39, Issue 3, September 2011, pp. 431-451
- Ilya Barabanov, Ivan Safronov & Elena Chernenko: *Razvedka botom [Intelligence Using a Bot]*. Kommersant, August 2012, <http://www.kommersant.ru/doc/2009256>, retrieved 7 November 2012
- Maya Bar-Hillel, Alon Maharshak, Avital Moshinsky & Ruth Nofech: *A rose by any other name: A social-cognitive perspective on poets and poetry*, *Judgment and Decision Making*, Vol. 7, No. 2, March 2012, pp. 149-164
- Ellen Barry: *Russian Lawmaker Quits After Real Estate Disclosure*, *New York Times*, February 21, 2013, <http://www.nytimes.com/2013/02/21/world/europe/vladimir-pekhtin-resigns-from-russian-parliament.html>, retrieved February 28, 2013

- John C. Bertot, Paul T. Jaeger & Justin M. Grimes: *Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies*, *Government Information Quarterly*, Vol. 27, Issue 3, July 2010, pp. 264–271
- Nick Fielding & Ian Cobain: *Revealed: US spy operation that manipulates social media.*, *The Guardian*, March 2011. <http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks>, retrieved 18 January 2013
- Freedom House: *Freedom in the World 2013*, 2013, <http://www.freedomhouse.org/report/freedom-world/freedom-world-2013>, retrieved 31 May 2013
- Keir Giles: "Information Troops" - *A Russian Cyber Command?*, 3rd International Conference on Cyber Conflict (ICCC), 2011, pp. 45–60
- Abraham H Maslow: *A theory of human motivation*. *Psychological Review*, Vol. 50 No. 4, 1943, pp. 370–96
- Li Baodong, Vitaly Churkin, Sirodjidin Aslov & Murad Askarov: *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, A/66/359
- Paul Meyer: *Diplomatic Alternatives to Cyber-Warfare*, *The RUSI Journal*, Vol. 157, Issue 1, 2012, pp. 14-19
- Robert Nozick: *Anarchy, State, and Utopia*, *Basic Books*, 1974
- Reporters without borders: *Internet enemies report 2012*, March 2012, http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf, retrieved 31 May 2013
- Paul Resnick, Ko Kuwabara, Richard Zeckhauser & Eric Friedman: *Reputation systems*. *Commun. ACM* Vol. 43, Issue 12, December 2000, pp. 45-48
- Robert T. Schatz & Howard Lavine: *Waving the Flag: National Symbolism, Social Identity, and Political Engagement*. *Political Psychology*, Vol. 28, No. 3, 2007, pp. 329–355
- Beth A. Simmons: *Compliance with International Agreements*, *Annual Review of Political Science*, Vol. 1, No. 1, June 1998, pp. 75-93
- Nassim Nicholas Taleb & Mark Blyth: *The black swan of Cairo*. *Foreign Affairs*, Vol. 90(3), 2011, pp. 33–39
- Torbjörn Tännsjö: *Understanding Ethics: An Introduction to Moral Theory*, *Edinburgh University Press*, 2002
- Transparency International: *Corruption Perceptions Index 2012*, <http://www.transparency.org/cpi2012/results>, retrieved 18 January 2013