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:

ISSN 1614-1687

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 "remailers", "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).