

December 2007

‘Online Identity’ affects real life? **The Changing Face of Identity**

A View on Risks and Guidelines associated with Online Identity

‘Know thyself.’¹

Our identity, our sense of self, shapes the world we live in and the world we create. As society becomes increasingly connected in this digital era in which we live, we more regularly overlap our offline identities with our online identities. This online identity is often difficult to precisely define as it is often defined by someone else's perception of the information available online about an individual. Understanding how identity's fluidity is increased online, and how to manage and shape it ourselves, creates an interesting topic worth of exploration. We find ourselves in a ubiquitous digital playground where bits and pieces of information about you and me are present, knowingly or unknowingly, willingly and possibly unwillingly.

Should you care? How does this affect our real life and can it be managed?

Our goal is to start discussion, illustrate perspectives and raise awareness.

This letter is the output of a 4-hour Expert-session on this topic, preceding the GovCert Symposium 2007 “Are you master of your own identity?”, Noordwijk aan Zee, The Netherlands. This first time internationally oriented Expert letter consists of contributions from the listed Expert-session participants, as a collaboration between the PvIB and GOVCERT.NL.

Page

2

BACKGROUND AND RESEARCH QUESTIONS

- Identity Online, Definition, Risks and Managing Identity

4

RISKS ASSOCIATED WITH ONLINE IDENTITY

- Which Risks Do We Face, Actual Incidents

11

MANAGING THE RISKS

- Risk Categories and How They Can Be Managed

16

GENERALLY APPLICABLE GUIDELINES

- This Is How You Should Manage Your Online Identity

17

CONCLUSIONS

18

OPEN ISSUES

Hong Gie Ong

Erno Duinhoven

Ben Elsinga

Joep Gommers

Marten Gorter

Aart Jochem

Leon Kuunders

Jeroen Laarakkers

Scott McIntyre

Rogier Posthuma

Kelvin Rorive

Eelco Stofbergen

Roelof Temmingh

<http://www.ibpedia.org>

<http://www.pvib.nl/>

• expertbrief@gvib.nl



¹From an inscription at The Oracle of Delphi

BACKGROUND

Universal right to protection of privacy

Protection of privacy is a universal human right. The universal declaration of human rights has a separate article on this:

“ Article 12.

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”²

The concept of "private life" is very broad and needs some clarification. In general a person's right to a private life means having the right to live one's own life with such personal privacy that is reasonable in a democratic society, while taking into account the rights and freedoms of others.³ The other way around, it includes that certain information about an individual is kept private and confidential.

Information and digital shadow

Information about an individual creates an identity of this person, tells who he or she is. Of course we have only one formal identity and laws regulate the use of this formal identity. Yet today we create an electronic identity in the myriad of databases used by government agencies, private corporations and other organizations by way we consume goods, utilize services, and through our many online communications. Several expressions describe the trail we leave behind, like 'e-footprint' or 'digital shadow' (that means the traceable data that a person creates by using technologies such as credit cards, cell phones, and the Internet; examples are cookies maintaining personal preferences when browsing the Internet, logs containing online behavior, profiling of online buyers, etc.). The question is how this affects us and if there is something we can do about it?

Practical implications

The existence of a digital shadow may have practical implications on my daily life, for instance on my reputation. No clear guidelines for online conduct are readily available. What do I advise my employees, colleagues or clients, what can I tell my family to do about their own privacy; should my mom go on MySpace/LinkedIn/FaceBook/BeBo/Hyves/....? What instructions do I give my children about putting information about themselves, family and friends online?

Good vs. Bad

We should not forget that online presence can give us many advantages; we experience this in our daily use of the Internet. Online Social Communities can give us many helpful services such as maintaining professional relations or keeping in touch with friends over time. This letter gives a broader insight in the awareness on not so explicit visible risks of online presence.

RESEARCH QUESTIONS

This leads to the main Research Question to be answered:

How can Online Identities influence real life and what control has the owner?

² See for complete text and context: <http://www.un.org/Overview/rights.html>

³ This clarification is stated in the 'Operational Guidance Human Rights Act 1998' of the British Charity Commission

The goal of this paper is to have an expert view on the topic; without the intent of spreading fear, uncertainty or doubt, but realistic and practical. To answer this main question, some additional questions must first be answered:

1. What is an Online Identity?
2. What are the risks associated with Online Identity?
3. Are there ways to somehow ‘manage’ Online Identities?

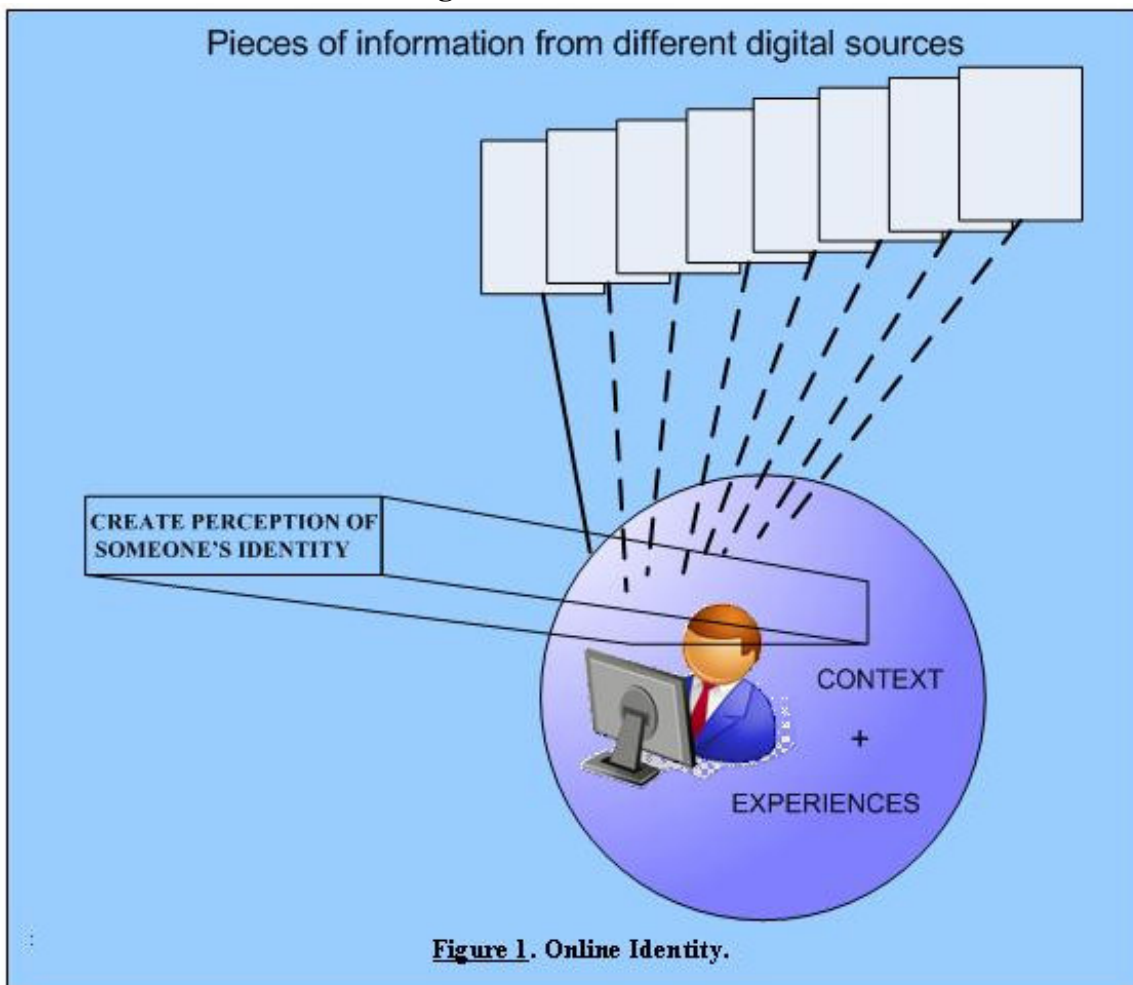
Definition

In this expert letter we will see that an Online Identity does not need to be built based on facts which can be proven. Nor does it have to be issued by an authorized agent. Summarized:

Online Identity:

A collection of digital information that gives us a perception of someone’s Identity.

Since *1 PNG > 1K Words*⁴, see **Figure 1** below.



Data from different, unrelated digital and non-digital sources, build up an image, a perception. This perception can change and is based on the context of the situation and experiences that the person or organization in the illustration has with possible previous (virtual and/or physical) encounters on his object. These sources could include a forum where comments were uploaded, Social Network communities, blogs, work related websites, (local) government information systems, membership-information and affiliations, newsgroups, photograph-, video-, and audio-sharing sites and possibly all other search engine results.

⁴ One picture says more than a thousand words ©
(thanks to Gigi Tagliapietra for his creative Symposium joke).

Also corporate or government databases add to the image of a person's Online Identity. Since different people have access to different information, a description of the object's Online Identity is always incomplete or subjective. **Identity is in the eye of the beholder.**

So far, it can be concluded, that Online Identity is a complex to grasp phenomenon, evolving and still in the process of being understood as proliferation of 'identity-particles' on different places on the Internet continues almost real-time. You yourself build up your own perception when for example checking someone's profile on a Social Networking site. You might think that's him, but what you **DO** with that information is interesting. We find ourselves in a digital landscape of infinite identity chess.

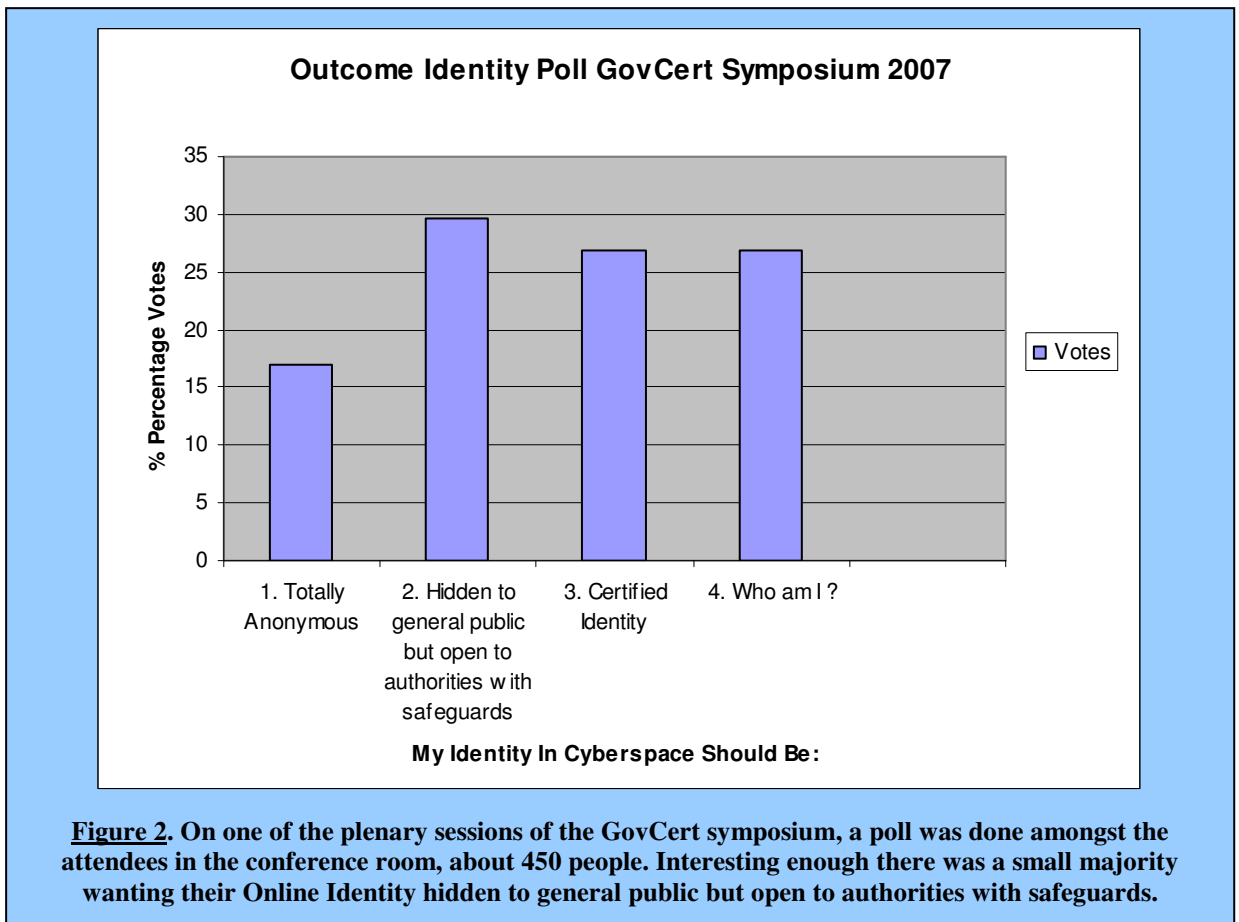


Figure 2. On one of the plenary sessions of the GovCert symposium, a poll was done amongst the attendees in the conference room, about 450 people. Interesting enough there was a small majority wanting their Online Identity hidden to general public but open to authorities with safeguards.

RISKS ASSOCIATED WITH ONLINE IDENTITY

Now that we shared some views on what Online Identity can be, we want to identify risks associated with this form of Identity. One issue we encountered was the many similarities



Figure 3. Impression of the brown paper session on identifying risks associated with unmanaged Online Identity.

between the risks for the unmanaged Online Identity, and the risks in traditional, or, "real life" identity. We will try to focus on the Online Identity.

We have identified many risks in having all kinds of information related to your Online Identity unmanaged online. Below you'll find an impression of the various risks that were discussed in the Expert session (see **Figure 3** for about 1/3 of the complete brown

paper collection), but on which we will not elaborate, since we will focus on what we

consider the main risks and where we believe through increased awareness, a real difference can be made.

Highlighted examples of risks considered:

Identity/Account Denial-of-Service

In some countries you still personally have to come to the bank to withdraw money. Say that you come there, but it appears someone prior to you was pretending to be you and tried to withdraw money in your name, which eventually led to the preventive locking of your account.

Public opinion manipulation and reputation

An identity defined by the characteristics mentioned before overlaps with what is called reputation, as the overall quality judged by people in general. This reputation can be manipulated by others. For example: create 1000 fake identities and go onto blogging/commenting negatively about government/company/person/product, influence public opinion.

Predict the future development of a person using Online Identity information

Putting data online is time-related, so one can often be tracked by what one places online and when; but also, maybe then they can predict future behaviour, resulting in scenarios as seen in the movie Minority Report.

Online Identity erasure

Once all Online Identity related information would be deleted, you cease to exist online, which possibly affects your real life; it seems at least, that no identity is completely analogue anymore.

Create an organization puzzle

Collect snippets of information from public available weblogs to create a more or less accurate picture of what is going on in an organization. Tools exist to match persons to organizations.

Focus on main risks of unmanaged Online Identity, where the most change is possible

The main risks of having an Online Identity unmanaged, as selected by our workgroup, are clustered in the following categories:

Category I. Characteristics of the Internet medium related to the Online Identity

- Not a 'stick your finger in the fire, then you'll get burned' environment, no direct feedback.
- Internet never forgets (mistakes); cookies, archives, logs; the way-back machine, Google cache, etc.; dismissing real life archive-related legislation.
- Ubiquitous presence and accessibility; everyone was/is/will be there.

Category II. Control of the information related to the Online Identity

- Nobody can hide
- Hard to control

Category III. Psychology of the Online Identity

- Wrong perception of Online Identity vs. Real Life Identity

Category IV. Misuse

- Impersonation
- Fraud
- Online Identity theft

We focussed on category I, II and III. We consider these to be the most differentiated ones apart from what is seen in daily risks related to the real world identity we already face. Things like identity fraud with passports have been covered in depth elsewhere; it's not less important, but the first three out of four categories are more related to our research questions and topic of exploration.

The categories of risks explained.

Category I. Characteristics of the Internet medium related to Online Identity

The Internet as a medium has characteristics that make it very useful for our every day work and private environment. In the context of this Expert letter however, we will focus on the downside these characteristics can have for our unmanaged Online Identity.

Environment/Sensory feedback

First, it is important to be aware that the Internet environment is in many ways a different world from the physical world we are used to. In our daily lives we can use our senses; hearing, seeing, smelling, tasting and feeling the things around us, which provide immediate signals for our brain that something is ‘good’ or ‘bad’ according to our common sense and experience. Consider a fire where you feel the immediate pain when coming too close to the flame; you’ll know to stay away. The Internet however doesn’t provide you with as many instant ‘stay away’, ‘don’t touch’ or ‘don’t-do-this-because-it-is-bad-for-you’ clues. Thus, on the Internet, few direct warning signals are present to explicitly stimulate our common sense, and rationale for making decisions of putting something online is still not part of our trained or daily habits.

Everything is documented

Extremely put: on the Internet, everything is documented or recorded. The time is not limited and in many ways data can not be permanently removed. Either the information put online has been copied onto other locations, data has been cached (e.g. search engine) or is still available through sites like the way-back-machine or likewise. Everyone can add some information. It has easy accessibility and correction of information once published onto the Internet is almost impossible. One would need thousands or millions of “delete-buttons” if information is on the Internet and you want it really removed.

Not one law applies to the Internet

The subordination to national legislation is limited and a lack of governance and **consistent** governance is a situation that the Internet currently faces; creating that consistency in legislation has repeatedly proven difficult, if not impossible. For instance the attempts by the European Union to harmonize legislation on data retention and the eventual (lacking) results. Storing personal information in real life is often subject to national legislation, while storing personal information on the Internet, which can be hosted in any country around the world, is regularly lacking clear jurisdictional controls. The world is still trying to map governance from real life onto the Internet, but the Internet cannot be mapped into traditional restrictive paradigms.

Reliability/Trustworthiness

The trustworthiness of information on the Internet is difficult to be determined and data validation is usually missing. Many assume that information presented on the Internet is reliable, but it isn’t. For most of the information out there, there’s just no way of knowing the level of reliability and there’s just no way to really validate information. We need to learn to handle uncertain and unreliable information.

All of the previous is even more interesting when put in another perspective. A famous saying said to be pronounced by Dutch writer Jan Blokker:

“History is not about what happened, but what people remember.”

As Internet presently functions as our global memory, we can actually change what people “remember”.

Some examples of incidents and anecdotes brought forward by the group of experts:

Being in control of your Online Identity is important for your own safety and security but also for everybody else. Terrorist cells are increasingly using the cybercrime to fund terrorism (does that make it semi-cyberterrorism? Read Adams, Dishman, McCaffrey, Basso) using creditcard fraud and emptying bank accounts. Not just funding, also using stolen identities to hide activities in the cyber as well as in unplugged life.

Example: Back in 2005 a foreign security company was assisted in pulling apart some artefacts, eventually aimed at convicting a known terrorist involved in bombings. It was an example of a terrorist who not only used cybercrime to fund his own activities but also urged other terrorists to hack into computer systems and steal credit-card data and other valuable intelligence. Our inability to correctly link (online-)identity and online services puts lives in danger.

Online raiders fool banks into handing over customers' details

..... the gang's favourite method was a process known as "account take over", in which the thieves got enough private information to convince a bank that they were the customer and then ordered a new card and PIN.....

"It may be that the criminals have been monitoring their victims and their habits and then used that information to use social engineering. People have to remember that there is no such thing as privacy in the online world."

<http://www.timesonline.co.uk/tol/news/uk/crime/article2759818.ece>

Google Interviewed

Google's overall goal is to have a record of every e-mail we have ever written, every contact whose details we have recorded, every file we have created, every picture we have taken and saved, every appointment we have made, every website we have visited, every search query we have typed into its home page, every ad we have clicked on, and everything we have bought online. It wants to know and record where we have been and, thanks to our search history of airlines, car-hire firms and MapQuest, where we are going in the future and when.

It does not simply want to be a good search engine on the web: it wants to be the web.

http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2688404.ece?print=yes&randnum=119295192115

New intelligence chief reveals all on website

<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/11/16/nbreach116.xml>

Category II. Control of the information related to the Online Identity

Taking into account the previous section about the characteristics of the Internet, we see the **control** of the information related to the Online Identity as another main risk of an unmanaged Online Identity. The Internet can be considered as a place where nobody can hide and the information is harder to control.

Online Identity information can roughly be tracked back to two sources. The first comprises information regarding ones Online Identity **from "official" sources**. "Official" means policy set by law, originated in real life. In real life, we're policed by law; things like Social Security Number, governmental arrangements, even library cards. We could call it Authoritative sources. The second source contains Information regarding ones Online Identity **from "unofficial" sources**. "Unofficial" means policed by society. The questions that arise here are the verifiability of the information. The uncontrollability of information from "unofficial" sources, could lead to risks such as:

- **No truth, no lies**

There's no truth on the Internet, but there are also no lies. Things just are.

You might want to control the past and influence the future, so you can understand the present. In our daily life, a normal way of conduct is the ability to present the truth based on context. A part of that context is of course also the exaggeration or slight bowing of the truth, in order to put what we say in line with our goal. In the world of IT as an example, it has become normal that a résumé is formed to fit the specific job description which is asked for. The Online Identity gives us a powerful tool to construct the image that is wished for by the future employer. Therefore that identity needs to be managed. Online, for every opinion and every viewpoint, a valid argument can be found. By "tying" those arguments around your Online Identity, the perception of your identity can be influenced. That perception or image created, is not necessarily true or untrue, but contextually driven.

- **Targeting collective identity**

When you find out which employees of a company maintain a weblog, it is possible to find snippets of social and business information regarding the company. Where the

individual snippets don't reveal too much, the aggregated information can provide a more or less accurate picture of the company

- **Identity farming**

Is collecting online identities a good or a bad thing? Or, more elaborate:

- **Data aggregation about ones Online Identity for possible future use**

With tools that aggregate Online Identity information from seemingly unrelated open sources, suddenly connections between parts of your relations (work, blog, memberships, affiliations, people connections multiple degrees away who are associated with unlawful actions) put things in a new perspective. Negative associations or your Online Identity linked to very personal information (phone-number, geo-location, school, hobbies) may seem harmless now, but could well be stored for future use and (mis)interpretation later.

- **Virtual identity manipulation**

You can assume a person's identity by registering free e-mail addresses in their name, setting up MySpace, Linked-In profiles as them and getting the identity "out there" so it gets indexed by Internet search engines.

There are even companies, which create a view **for** you; it gives you the ability, to say: these unofficial information sources are verified by me. These companies obtain that information from the society and the Internet itself, giving **you** an opportunity to create and shape your own identity profile. If somebody else creates a profile for you, then you have to contest that and say "that's not me", these are the reasons why it's not me and it gets harder and harder if someone is desperately trying to impersonate you.



We were trying to see if there is some sort of balance possible or even necessary between being totally anonymous vs. full exposure of your Online Identity information. If you're totally anonymous, then they can recreate you easily, since there's no information about you online, so everything can be made up.

If information regarding your Online Identity is fully exposed, they can recreate you really well, because all the information there is to know is available about you. We don't know which situation is the best, but we leave it for further discussion.

- **Absence of social boundaries on the Internet**

An important aspect in relation to control over information online, is that the social control as it exists in real life is largely absent on the Internet. Possibly this, on the other hand, explains the popularity of Social Networking sites such as MySpace, Hyves (Dutch) and FaceBook.

In any case, the absence of social boundaries on the Internet, creates a grey area for what is or is not acceptable "behaviour" of putting something online about ones Online Identity.

- **Subjective interpretation of search engine results from official or unofficial sources**

Most people look at only the first page of Google results; do Google indexing results define my Online Identity? This makes it possible to influence an Online Identity by manipulation of indexing results. It already happens with commercial interesting search words, so why not with social interesting search words? Would this make you think twice about interpreting Search Results?

Google Adwords and Google Alerts

You can already pay Google to have your ad come up next to the search results on a topic or word related to your business or personal preferences (**Google Adwords**). So you know how often your identity for instance is searched, or what kind of description is shown upon the trigger.

Using **Google Alerts**, you can set your preferences in such a way, that when something about your Identity is put online and indexed by Google, you receive an e-mail so you know what is known about you online.

Addressing the same category of risks, there are companies that provide online Reputation management systems (e.g. www.rapleaf.com) or companies you can pay for erasing data in online databases all over the world (various commercial sites). An old Chinese proverb describes the caveat best: *“Reputation comes on foot and leaves by horseback.”*

Some examples on actual incidents and online stories:

Online criminals target Facebook and virtual worlds

Social networking sites and other online communities are being mined for personal information, a report warns. Organised criminals are increasingly targeting online communities such as social networking sites and multi-player computer games, a security report has warned. The vast amount of personal information stored on sites such as Facebook has made them a rich source for fraudsters, who use the details to create highly specific threats "There is an increasing trend towards attacks on social environments like Facebook and LinkedIn, where the quality and quantity of private information is such that attacks can be more focused."

Having read a Facebook profile, a fraudster sending a subsequent e-mail could, for instance, address the recipient as a lawyer, and make reference to events they have attended, giving the message an air of authenticity,

http://technology.timesonline.co.uk/tol/news/tech_and_web/article2474779.ece

Misunderstood

Another example on managing your Online Identity was published in the NYtimes http://www.nytimes.com/2007/10/25/science/25jacobson.html?_r=2&oref=slogin&oref=slogin. It is the story about the 84 year old scientist Homer Jacobson who Googled himself and found out that an article from the American Scientist he wrote in 1955 was used by creationists as scientific proof that the early earth could not have contained amino acids, the building blocks of life. He decided to withdraw the article, 52 years after it was published.

Signs of the social networking times

<http://www.geekculture.com/joyoftech/joyarchives/1041.html>

Category III. Psychology of the Online Identity

- Wrong perception of Online Identity vs. Real Life Identity

In another subsession of the expert meeting the psychological aspects of having an Online Identity were discussed. The discussion is captured in a diagram, shown in **Figure 4**.

This section describes the outcome of the psychological subsession of our expert meeting.

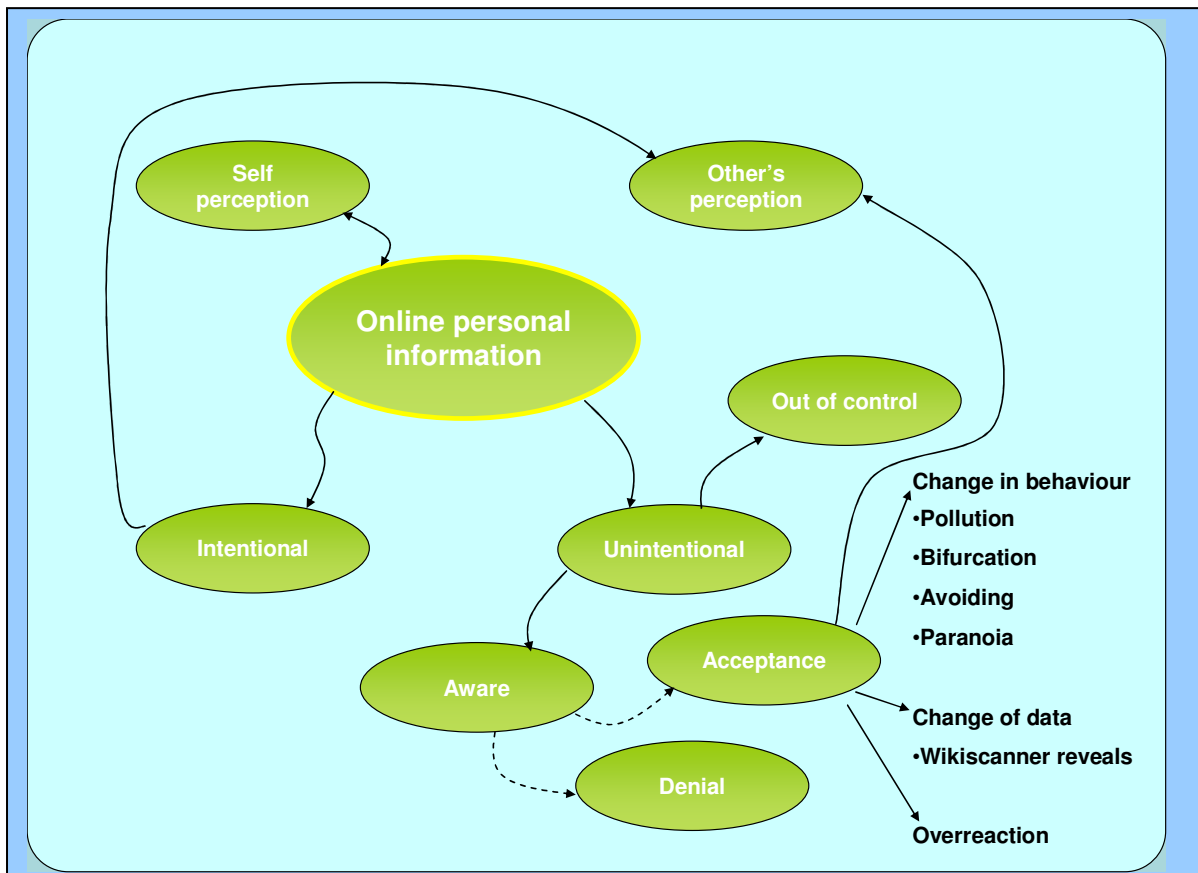


Figure 4. Psychological aspects of online personal information.

A brief explanation is in order. The expressions in **bold** in the elaboration that follows, refer to the keywords in **Figure 4**.

As previously stipulated, Identity is the summation of information about an individual both offline and on. With respect to **online information**, data can either be **intentionally** contributed by ourselves (such as our home “home page” or profiles on Social Networking sites) or **unintentionally** (externally) contributed through the words and acts of others. Externally contributed data is often felt to be beyond our control; a sensation itself which shapes our Identity.

This information then acts upon our own **self perception**, as well as **other’s perception** about us. In essence, this creates a feedback loop and plays a role in shaping our Identity and perceptions about our Identity.

When the person becomes **aware** of this (unintentionally contributed) information he or she can **deny** the existence of the information or **deny** that it is connected to him or her. Whilst this may seem like a familiar coping strategy, in the end it has little effect on the core issue of the perception of Online Identity; the data and information is still “out there” and perceptions are still formed, despite our **denial**.

The other option is **Acceptance**, which can lead an individual to undertake one of three primary responses: **change in behaviour**, **change the data**, or, more extremely, **overreact**.

Changing behaviour itself can take many forms, such as providing minimal information on the Internet in web-forms, avoiding the filling out of “optional” data fields, no longer participating in those communities where the unintentionally contributing information was sourced from (providing a vehicle for opinion and perception change in others) and so on. A slightly more subversive behaviour change would be to start **pollution** of databases (using different Identities such as shopping cards used for tracking shopping habits) with the simple goal of Identity obfuscation.

When confronted with too much intentional data shaping other’s perception of our Identity, another potential reaction could be **paranoia**. Understanding and integrating the many types of data affecting Identity can be a daunting task, and the nature of Internet Identity may render one in a state of near-panic brought about by just how much data can be amassed and shared online, without our direct involvement or desires.

Acceptance can also lead to try to **change the data** involved (data protection regulations provide some assistance here). Stories involving **Wikiscanner** disclosing the true sources of information alterations at Wikipedia concerning Dutch Royal backgrounds created an upset in the Netherlands.

In extreme cases, confrontation over one’s intentional and unintentional Online Identity can lead to **overreactions**, such as threatening others and trying to regain control over your Identity through unusual (and often physical) methods. When one feels that their Self-Identity is beyond their locus of control, they may feel compelled to take drastic action to resolve the internal/external conflict. Recent news events have highlighted the specific vulnerability that the younger generation faces here, and how the results of “online bullying” can so drastically shape one’s sense of self that depression and even suicide have been the result.

This leaves us with the final event following the Acceptance, the so-called **Bifurcation of Identity**, meaning a split of Identity definition; a decision-making point. This affords us the

opportunity to accept a series of intentional and unintentional information elements at a specific point in time, but create a new “branch” of our Identity to move forward with. One could say to that employer who didn’t offer us a job due to their interpretation of our Online Identity: let’s correct that and let’s move on. This is, in essence accepting the history behind you, accepting that it exists and **using** that identity to regain control for your own goals.

Every time we accept that an unintentional interpretation of our Identity has taken place, we have an opportunity to use that information and change direction. This can happen to your Online Identity any number of times, and even intentionally, such as when we create a new Online Identity to participate in a new online environment (game, forum, Social Network).

It’s therefore safe to say that there is no such thing as a single Online Identity, or a single professional Identity. Each-time you have accepted that unintentional interpretation of information on your Online Identity has taken place, you have the opportunity to mark a change and give yourself control again.

Whilst it may seem there is no obvious conclusion to be drawn here, further discussion brought about the awareness that these conscious manipulations of our behaviour with respect to Online Identity helps to re-shape the perceptions others have of our Identity, and therefore our Identity itself.

Example from the real world:

A very simple example is the rating system of sites like E-bay and BOL, which are used to define (or try to define) some levels of trust within Online identities. That level is a mix of Online Identity and identity: there they are really intermingled. Examples on how to hack these trust-systems or on the concerns there are on how to protect Online identities from specific attacks targeted at their trustworthiness can easily be found.

MANAGING THE RISKS

After we have tried to analyse the risks associated with Online Identities, we turn our focus to possible ways to manage these risks. In this section we will discuss possible ways to manage the risks per category.

Managing risks of Category I. Characteristics of the Internet medium related to the Online Identity.

This category includes lack of sensory feedback, the full documentation of your actions, the lack of consistent online governance and the reliability and trustworthiness of information on the Internet. Since as an individual, we cannot change these characteristics, we should take responsibility as an individual and also as a collective, and accept the described characteristics of the Internet medium.

The rational first step would then be to identify what is there regarding the presence of your Online Identities. A helpful tool in the form of an ID-Radar is put forward as an example to make an inventory of sources of Online Identities.

Factual vs. Fictional / Subjective vs. Objective: Everything is documented

Most people can likely relate to some parts of it, if not to all quadrants, but this model summarises many of the loci of Online Identities (**Figure 5**). Most employees have a work-related e-mail address, based on the factual situation; you have a formal name and work for a certain company, thus factual composition of the mail-address. The private quadrant with pseudo names gets more interesting. In virtual environments, online games, chat-rooms and so on, Identities tend to get more fictional, thus to the outside of the circles of fact vs. fiction. The outer Identities have little effect on the factual identity, as long as they stay in the outer circles. The more info related to the person is released through the fictional ID, the more it drifts to the center.

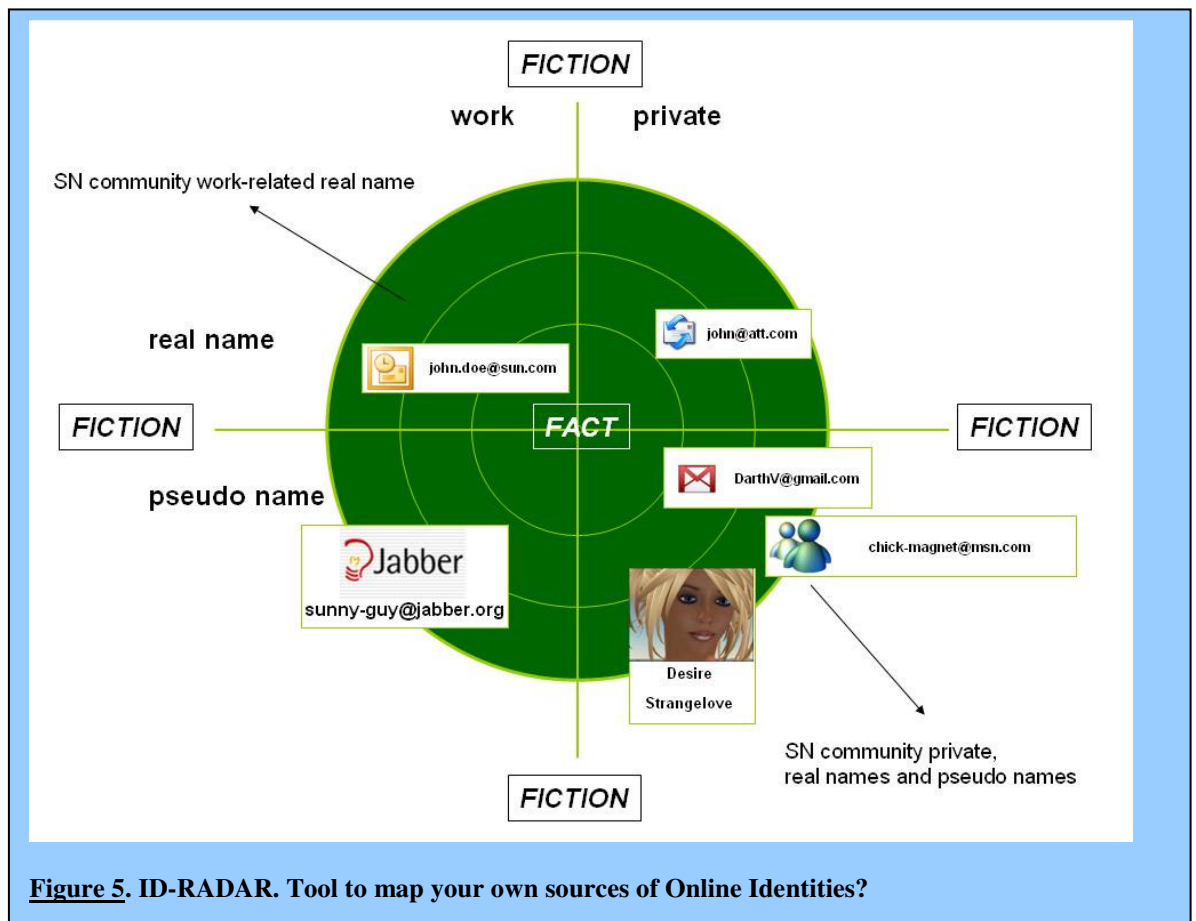


Figure 5. ID-RADAR. Tool to map your own sources of Online Identities?

An example is when a connection is made between a pseudo name and the person through so-called *Exif*⁵-data of published images, which is added by your digital camera when the picture is taken.

The only way to manage the risk of these Internet characteristics is by realizing that whatever information you publish on the Internet is there to stay. Think before posting information to the Internet. Unfortunately there may also be other people that publish information on the Internet regarding your Online Identity. You can do two things. Periodically check through search engines what information is available on the Internet regarding your Online Identity. And, whenever you know someone is publishing something about you on the Internet, try to be able to influence whatever is published on the Internet.

Actions needed to resolve issues caused by the lack of consistent online governance

- Government and commercial organisations promote the use of electronic media (and its characteristics described), so they should take responsibility to minimize the associated risks of misuse of Identities of online citizens and clients. The impact on society is big. Data protection rules should be formulated where needed and enforced by an authority with some power.
- A form of police analogous to real life police is necessary, most probably a high tech team of existing police corpses. Today criminal activity remains unpunished and citizens are not understood when they report Identity theft. An example is the fraud on E-bay and known cases of Online Identity-theft. We need someone to fight that situation.
- Individual responsibility can be brought about through awareness and education.

⁵ Exchangeable image file format (Exif) is a specification for the image file format used by digital cameras. The specification uses certain file formats, with the addition of specific metadata tags.

The presence of an authority/regulator/police on the Internet, led to some fierce discussions. It can only be noted that some of us don't believe in regulations in combination with the free medium of Internet, and some of us do. No conclusions can be drawn from the argument battle and we didn't get to the physical battle (also time ran out).

Managing risks of Cat. II. Control of the information related to the Online Identity.

This category includes the fact that there is no truth nor lies on the internet, the risk of targeting a collective identity, identity farming and deliberate collection of fragments of information, the absence of social boundaries and manipulation of search results.

There is always an Online Identity; there's no such thing as not having an Online Identity, so accept it. That's the first step in being able to manage the risks in having an unmanaged (uncontrolled) Online Identity.

It is too easy to say people should simply use their common sense in controlling the information they put out there. People are simply incapable to analyze information, evaluate risks, relate threats and see possible chain-reactions and consequences (impact). Nonetheless, the overview of the risks related to the characteristics of the online environment as opposed to the real life environment already backed the use of warning messages through real life analogies. We should apply absolute risks where possible and communicate properly⁶:

Tell kids not to walk or cycle through red light, because they don't know the risks what can happen. Also brushing your teeth is not a natural habit, but learned by every day attention of the parents until it becomes a habit. The same is true for putting information online regarding ones Online Identity. Educate them!



The boss used his "common sense" and come to the conclusion to decide not to hire that potential employee, based on the "factual information" that he encountered online. Common sense is what got us into this problem in the first place. So it is difficult to trust the very thing that has been broken.

- Educate public awareness, help them understand the importance of thinking critically and then their common sense can be of help in managing the risks.
- People should be taught how to be more alert.
- Raise the 'Stick your finger in the fire and you'll get burned' experience. Teach people to think differently and react differently because of the different nature of Internet and how information is to be controlled in a virtual world. An example of feedback is to leave your e-mail address somewhere and receive spam.
- Policed by law could take years. Policed by society takes immediate effect.
- User education, maybe from official source; this is how it works, even at school level, we have to tell the public "this is it how it works online, specifically from an Identity point of view."
- Work on verified Identity

⁶ Absolute risks and communicating properly was in the presentation by Urs E. Gattiker, Ph.D., one of the GovCert Symposium speakers on why all Security Awareness initiatives have failed and continue to do so. Most security awareness initiatives do not address the effect of such factors as: gender, age, knowledge level of users, etc.

Managing risks of Cat. III. Psychology of the Online Identity

This category includes the risks of self-perception vs. other's perception, and Acceptance vs. Denial.

Lot of companies have privacy policies and guidelines, but it takes lots of energy to make the users aware. Acceptance and understanding seem the only rational way of mitigating any risk caused by psychology of the Online Identity.

Tooling

According to "If you don't know what you have, you don't know what you're missing", it seems a rational first step to know yourself what's known about you. There are various online tools, for example Google of course, what we could call the *Perception of Identity Tool* (**Figure 6**) since it creates a perception (also see **Figure 1**):

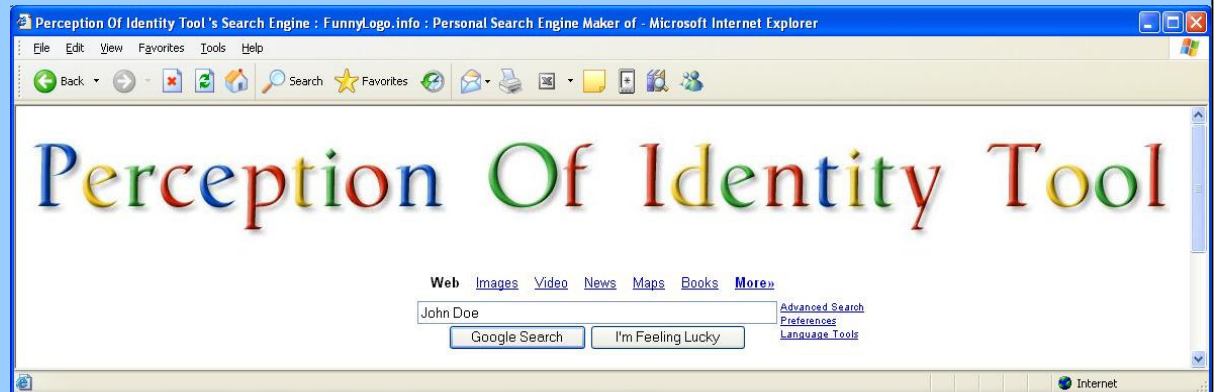


Figure 6. Google search, creating a perception of identities.

More advanced tooling; another perspective: **MALTEGO**
 Maltego is a program that can be used to determine the relationships and real world links between:

- People
- Groups of people (social networks)
- Companies
- Organizations
- Web sites
- Internet infrastructure such as: Domains, DNS names, Netblocks, IP addresses
- Phrases
- Affiliations
- Documents and files
- These entities are linked using open source intelligence.

Find 'hidden' relationships. A=>B=>C and X=>Y=>C ...then A = ~X

"Google is a great first stop for many searches, but it doesn't provide relational links to reconstruct a person's (or organisation's) entire web-presence, including their relationships with other subjects and resources."

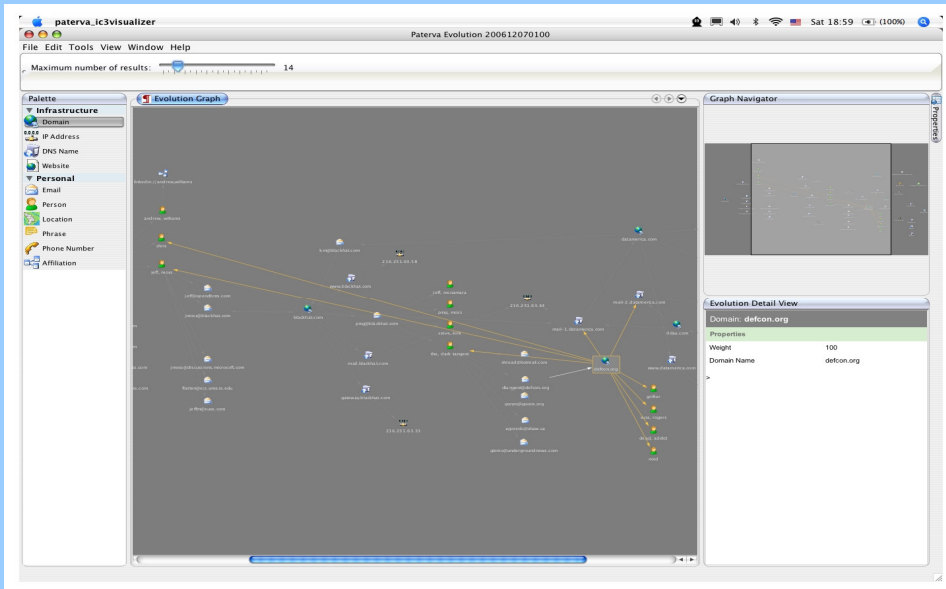


Figure 7. Maltego. Relations become explicit.

It translates *entities* such as a person's name, a domain name or e-mail-address to other *entities*, thus, relations become explicit. Pieces of the puzzle that reflect your Online Identity become visible on stage. Search Results are visualized and connected as can be seen from the screenshot (**Figure 7**) shown of a web-address of an organization being analyzed.

Here are some examples of translations, the so-called *Transforms*:

Transform	input	output	Description
To Email Addresses	PhoneNumber	EmailAddress	This transform searches for the telephone number and returns related email addresses
Parse Meta information	Document	Person, Mailaddress, Phrase, Documents	This transform extracts the meta information from the document and then parses it for username (persons) and/or email addresses.
To Rappleaf Affiliation	EmailAddress	Social Network Memberships, Person	This transform will see if the email address exists on Rappleaf. It will then show all social network memberships it can find.
To DNS Name	Person	DNSName	This transform shows sites where various permutations of the person's name was found.

The information is already there on the Internet, just nobody thought about tying the dots together, creating a more complete subset of an Online Identity collective. The example represents an organization (example taken from a previous Defcon-symposium presentation of one of the Expert-session participants). Currently already **60+** (!) *Transforms* are available and due to public source-code, everyone can develop and add a *transform* (as we speak). The relations/connections in the graph continue to grow and the subset of an Online Identity is becoming extensive.

GENERALLY APPLICABLE GUIDELINES



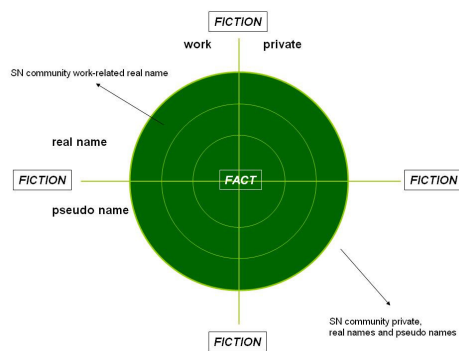
Understand the other world vs. the real world

Realize and accept not having a “Stick your finger in the fire and you’ll get burned” environment. Educate.

Be proactive, Make a choice; Think About It

You either want to be completely anonymous or don’t care what information on your identity is known out there.

Create a balance of what is rational to you.



Make an Inventory; Be Aware

Such as the ID-RADAR, to know your primary means of E-footprint leaving identities at least and possibly their ‘weight’ and map out your own perceptions of your Online Identity.

Take Responsibility; Purpose Driven Identity

In the pile of ubiquitous Online Identity information that’s building up, at least take your own responsibility as an individual and control your pieces of information. Define your own set of information you want to put online, based on the goals you are trying to reach with your Online Identity exposure. Have you considered the purpose of exposure vs. the possible consequences? Raise the bar for the average Joe to make a connection between you and a pseudo-name if that is your goal.

Know what is known online about you

If you want to understand the perceptions of others; recruiters, potential employers, friends, family, acquaintances and strangers, you might want to know what is known online about you already.



Act Rational as you would in Real Life

You are always able to respond to a perception or misperception of your Online Identity. It seems to be impossible to remove false or unwanted data from the internet, but you can. Data protection authorities in several countries (UK, NL) have guidelines to do this.

CONCLUSIONS

We enjoy the advantages of having an online Identity everyday as we surf the Net, e-mail or chat on a social or even corporate level. What we are trying to put forward in this letter, are the considerations we should have as a responsible individual. It is important to note that the perception of the information regarding our Online Identities can indeed be influenced, thus also our real life experience of that perception by someone.

To answer our research questions:

1. What is an Online Identity?

A collection of digital information that gives us a perception of someone's identity.

2. What are the risks associated with Online Identity?

A multitude; we touched some of them in this letter. We categorized them in "The Characteristics of the Internet", "Control over the Information related to our Online Identities" and "The Psychological Aspects".

3. Are there ways to somehow 'manage' Online Identities?

(Can we somehow be more proactive in building an Online Identity? Which means are there to influence Online Identity, are there on-line tools?)

We can manage Online Identities, by being aware of the environment we put information about our Identity in and acting rationally. The analogy has been made about the Internet not being an environment such as real life, where you put your finger in the fire and you'll get burned. Other rationales are thus necessary to call upon.

And finally to answer our main research question:

How can online identities influence real life and what control has the owner?

As communication means have developed, people have found ways to express themselves in multi-faceted ways; there is no such thing as **ONE** Online Identity, you have a myriad of them depending on the environment you're interacting with. The psychology paragraph of this Expert letter helped to argue this and illustrated how indeed our real life can be influenced by our Online Identities and the unintentional perceptions thereof by others.

You can influence your Online Identity by being more aware of how it can be interpreted. Consider the consequences and evaluate. Different tools are available to either help you to know what is known about you, for you or someone else, or to an evil-minded individual. It's important to realize that. We must be aware 'our finger can get burned'.

We think we reached a better view on the scope of the problem by having this session and its outcome expressed through this letter. We're more convinced than ever that **awareness** is important. Awareness in the new risks involved in unmanaged Online Identities and what can be done about it.

The new generation of Internet users seems not to be privacy aware.

Are **you** master of your own identity?

OPEN ISSUES

- What is the role of government and what measures can be taken to make internet a safer place for social behaviour and networking? How far must regulations go and when is self regulation by ISPs and the online branch possible?
- Balance between Total anonymity vs. Full Exposure of Online Identity. Feasibility, User friendliness, Functionality: triangle of research
- Many aspects of Online Identity being told were very personal; still the Corporate Online Identity can be more in-depth. Take it up to the level of businesses. Corporate stakeholders vs. privacy stakeholders.
- Chicken or Egg – E-Footprint or Online Identity. Is Online Identity created by the E-footprint or is the E-footprint created by having an Online Identity. What would the conclusion imply? This requires research.
- Effects of Mobile Identity in near future; analogy: at home you can regulate Internet use through proxy and so on, but these days 10 or 11-year old kids have cellphones with online MSN, and you can't control that device; they have it with them everywhere. If you take the device, they'll just get another device. Seems like education is the only way, but further discussion should be interesting.

REFERENCES

[x] GovCert Symposium 18-19 October 2007 ‘Are you master of your own identity?’

[x] All URL’s/referrals mentioned:

Universal Declaration of Human Rights on The Protection of Privacy:

www.un.org/Overview/rights.html

The WayBackMachine – Internet Archive:

www.archive.org

Social Networking examples:

www.myspace.com

www.facebook.com

www.linkedin.com

www.hyves.nl

www.bebo.com

People Search examples:

www.google.com

www.spock.com

www.wieowie.nl

www.zoominfo.com

www.wink.com

Reputation Management example:

www.rapleaf.com

Advanced People/Organization Search example:

www.paterva.com/web2/maltego/maltego.html

Organizations who made this Expert Letter possible:

www.pvib.nl

www.govcert.nl

Further reading:

<http://www.thoughtleader.co.za/bertolivier/2007/11/27/the-changing-face-of-identity/>

Quotes to think about:

“THE VALUE OF IDENTITY OF COURSE IS THAT SO OFTEN WITH IT COMES PURPOSE.”

- R. GRANT

“THE KEY TO GROWTH IS THE INTRODUCTION OF HIGHER DIMENSIONS OF CONSCIOUSNESS INTO OUR AWARENESS.”

-LAO TZE

“LIFE CEASES TO BE A FRACTION AND BECOMES AN INTEGER.”

-HARRY EMERSON FOSDICK, ON BEING A REAL PERSON

“THERE IS NO TRUTH, THERE IS ONLY PERCEPTION.”

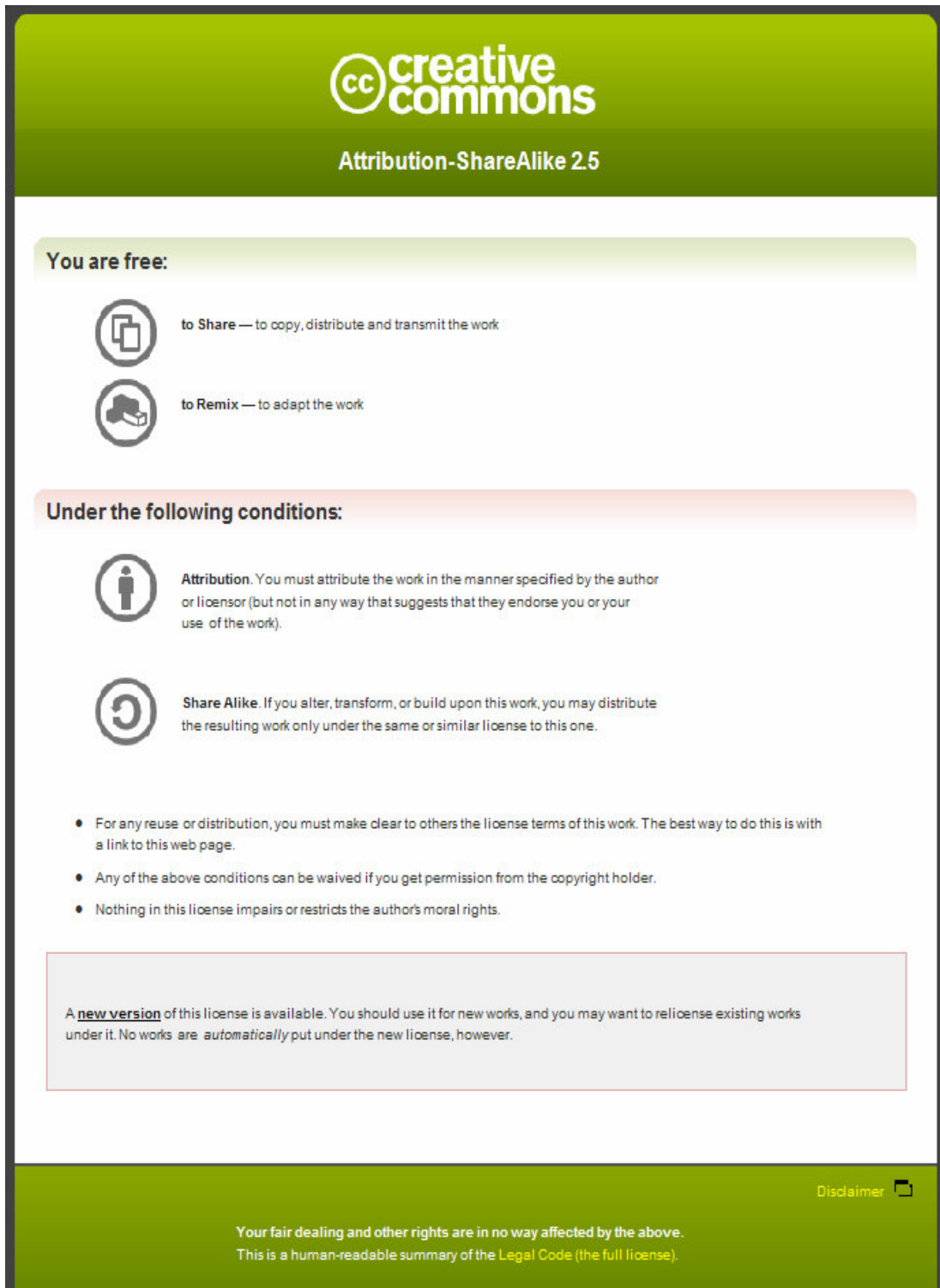
- GUSTAVE FLAUBERT

Annex: Applicable licence

The expert letter is published under the following licence:

<http://creativecommons.org/licenses/by-sa/2.5/>



At the time of writing, this page appears as follows:





The image shows a screenshot of the Creative Commons Attribution-ShareAlike 2.5 license page. The page has a green header with the Creative Commons logo and the text "Attribution-ShareAlike 2.5". Below the header, there are two main sections: "You are free:" and "Under the following conditions:". The "You are free:" section includes two icons: a share icon (two overlapping rectangles) and a remix icon (a hand holding a pencil). The "Under the following conditions:" section includes two icons: a person icon and a circular arrow icon. Below these icons are detailed explanations of the "Attribution" and "Share Alike" conditions. At the bottom of the page, there is a disclaimer box and a footer with a disclaimer icon and text.

creativecommons
Attribution-ShareAlike 2.5

You are free:


-  **to Share** — to copy, distribute and transmit the work
-  **to Remix** — to adapt the work

Under the following conditions:

-  **Attribution.** You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).
-  **Share Alike.** If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

- For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this web page.
- Any of the above conditions can be waived if you get permission from the copyright holder.
- Nothing in this license impairs or restricts the author's moral rights.

A [new version](#) of this license is available. You should use it for new works, and you may want to relicense existing works under it. No works are *automatically* put under the new license, however.

Disclaimer 

Your fair dealing and other rights are in no way affected by the above.
This is a human-readable summary of the [Legal Code](#) (the full license).

JOIN THE PvIB, FOR SAFETY AND SECURITY ...



Information security has been an essential and exciting subject for many years. Almost all occupations are having to place more emphasis on the confidentiality, availability and integrity of their information. Whether you are a CISO, manager, consultant or programmer, the Platform for Information Security (PvIB) can help you with information security issues.

What is the Platform for Information Security?

The PvIB is an open, broad-based association for professionals to build a more professional approach to information security, through the exchange of ideas, information, knowledge, insights and above all, practical experience.

What are our aims?

We aim to promote the physical, systems and organisational security of data and data processing equipment against in-coming and outgoing breaches. We also promote the exchange of knowledge and experience and the networking of practitioners in the sector - through this Expert Letter, for example.

Our target group

The target group for the PvIB includes everyone involved in information security, either as a student or professionally, or who are especially interested in the field. Our rapidly growing membership covers many different disciplines: students, information architects, technicians, managers, organisational consultants, legal specialists, security officials and ICT auditors. Our members come from all kinds of educational backgrounds, companies, public authorities, organisations and suppliers.