Think you know everything about identity protection?

Copied from www.socialmarketresearchforcharity.org/index3a.html#identity

The topic of "Identity Protection", covering real and social identity(s), includes monitoring, alerts, credit & content freezes (limited access), reimbursement insurance, digital identity/ resolution, restoration, reputation management (this category; primarily for businesses), and "best-practice" advisories - requires a multi-step introduction, as this exploratory discussion reveals **the un-met, compelling** need for 'social web services' that:

> "**Help protect everyday people's social (and real) identity(s); Focuses on the elements of social fraud, resolution & negative content;** While generating personal, social & philanthropic value from people's everyday social content, for worthy social causes; The analytics of which, entice sponsors to precisely match people's qualified (validated by their social discussions), personal and philanthropic interests; delivered non-invasive on-demand --- e.g. *Without the risk of being associated with any identity content about a qualified prospect,* SMRC will generate **100% personalized promotional research opportunities** (goodwill & rewards-based, précisely matched to each person), delivered on demand (browser extension), as well as through a sponsor's site (i.e. SMRC sponsors can produce 100% personalized, 1st or 2nd party, precise promotion via OpenX). No cost to register. No purchase is required.

SMRC's identity discussion is presented as a series of subject categories that are expanded upon in the pages that follow. Respectively, the first layer of the presentation is below. On the website, the links (underlines) expand the sections, whereas with this document, it is only necessary to go to the next page(s).

IDENTITY - Social and Real Protection (out of profile activity - preventative identity protection):

I. **How it Works** (Page 2): While protecting each person's identity (for their *authorized* content, even from SMRC, with unbreakable one way encryption & biometric security), the service can monitor all public social content, for suspicious out-of-character/ profile activity, associated with either with **(A)** one of the member's **social identities,** or **(B)** the member's **REAL identity** (as name, SSN, phone, address, email or other reference). Understanding the emotional character of content, **SMRC can also monitor for 'negative' (dislike) content, that references each person's (or brand's) real or social identity(s).**

II. **SMRC's *Approach* to Identity Protection** - (Page 2) **The problems and the solutions** from monitoring EVERYTHING, to alerts from in-depth profiling, to best practice resolutions (fixing problems):

III. **Market (Competitive) *Approach* to 'Identity Theft Protection'** (Page 2) - from protection of your *'Real Identity'* (financially) to distinguishing between others with the same name (e.g. *Digital Identity*) to *'Reputation Management' - the full story (fear; numbers/percentages; real identity; 1%/ households):* ***Everything you need to know about identity protection market offerings.***

IV. **SMRC's *Preventative* Identity Protection Services** - (Page 3) **about early warning: monitoring & alerts; all topics; in-depth comparative profiling:** By contrast, SMRC's services are designed to be preventative, filling in the missing searches that catch problems before they happen, ***for real and social identity(s), scoping all topics in discussion, as compared to just purchases or bank accounts.***

SMRC addresses the four (4) types of problems "associated" with identity protection:
(1) Real Identity Fraud, (2) Social Identity Fraud, (3) SPAM, and (4) Negative Content.

V. **The *Effective* Cost of Identity Protection** (Page 5):

IDENTITY - Social and Real Protection (out of profile activity - preventative identity protection):

I. How it Works: While protecting each person's identity (for their *authorized* content, even from SMRC, with unbreakable one way encryption & biometric security), the service can monitor all public social content, for suspicious out-of-character/ profile activity, associated with either with **(A)** one of the member's **social identities,** or **(B)** the member's **REAL identity** (as name, SSN, phone, address, email or other reference). *Understanding the **precise** emotional character of content, **SMRC can also monitor for 'negative' (dislike) content, that references each person's real or social identity(s).*** This is only possible based on in-depth, ongoing profiling (covering all topics, with friends and followers, over years) that knows exactly what topics each person really dislikes, along with the topics each person really likes, validated/ confirmed further by their reference to each topic in their ongoing social discussions. **Each flagged incident** will include a link to the referenced media item/ artifact with this optional service.

II. SMRC's *Approach* to Identity Protection - **The problems and the solutions** from monitoring EVERYTHING, to alerts from in-depth profiling, to best practice resolutions (fixing problems)**:** Because of the redundant nature of the Internet (which insures it stays up), that backs up and re-distributes 2nd copies of everything (e.g. like the 'Wayback Machine' [web.archive.org], Torrents, rss, blogs, search, archives, groups, etc.), **it's impossible to 'protect' each person by attempting to lock up content.** By contrast, the 'best practice strategy' (process) is to **aggressively** monitor the Net for potential harmful content that is apparently related to the individual's real or social identity(s), and to **aggressively** respond based on the type of problem - e.g. identity fraud or negative comments related to the member's identity(s). **For solutions,** see "Solutions for Identity Problems", under 'SMRC's Related Security Policies' below.

The total range of invasive social media related problems that SMRC will address can be seen **HERE**.

III. Alternate /Market Identity "Theft" Protection (fear) *Approach*: - from the protection of your *'Real Identity'* (financially) to distinguishing between others with the same name (e.g. *Digital Identity*) to *'Reputation Management' - the full story (fear; numbers/percentages; real identity; 1%/ households):* ***Everything you need to know about identity protection market offerings***

- **SMRC's Identity Protection *Non-Compete Disclaimer* (SMRC provides assurance and scope, not insurance):** SMRC's identity protection is not in competition to current 'identity protection services' (although its' findings will most likely overlap), whose services are typically limited to **(1)** monitoring your credit reports, **(2)** profiling your critical identity information (e.g. SSN, bank information, your name, etc.) across the Net, file-sharing sites, and financial networks, with a focus on monitoring for new saving and checking accounts in your name, and **(3)** providing bonded 'guarantees' of protection (or built in limits on liability, for example on Internet transactions). Furthermore, some services work directly with the credit card companies, to settle fraudulent accounts. **Identity theft protection plans, in total, address (a)** monitoring, **(b)** fraud alert, **(c)** credit freeze, **(d)** reimbursement insurance, **(e)** resolution and **(f)** restoration.

- **Their Value:** Most of these services are also provided by many banks and financial institutions (including insurance companies) for a fee or at no cost for being a member. Similar to other forms of insurance, **they mostly all offer acceptable risk vs. returns, but can't stop the problems from occurring,** as with the many fraud cases associated with Lifelock's promotion (e.g. 13 major cases, involving $million+ of fraud). **Respectively, if you're looking for 'identity protection *(reimbursement) insurance*' that includes *monitoring for new bank accounts that SMRC can't see/monitor*** (as they are secure and not publicly available except in your big agency credit report), or ***services that work with the credit card companies to settle fraud (resolution/restoration),*** you should get it from your bank or one of these services.

- **The Real Story (It's Not that Big a Problem): While 9 million (or 2.7% of the population)** people fall victim to identity theft (socially and financially) each year, **allowing identity protection company marketing to make heavy-handed claims** like *"One of the fastest-growing crimes"; "9 million Americans fall victim"; and "You could already be a victim.",* **less than 1 percent of households reported** someone opening unauthorized credit, stealing their tax refunds, or tapping into their medical benefits, according to the U.S Justice Department. *The main service that these companies offer is monitoring the big credit bureaus -- Experian, Transunion and Equifax -- for new credit requests in your name. But you can do that yourself.* Of the **~37 million articles on Google related to 'Identity Theft Protection',** the general recommendation is to **get an annual credit report from each of the three reporting bureaus.** It's free, and if you stagger your requests, you can get a fresh report every four months.

- **The Social Identity Story (Is a Big Problem)**: While less than **1 percent** of households reported **"real identity fraud"** (bank, taxes, benefits fraud), social identity problems pose the greatest threat to 'Millenials', **affecting over 30% of Generation Y**, age 16-35 annually, as reported by the Associated Press, **that includes (a)** spoofed/hacked accounts (primarily from people either sharing their passwords, or as stated before - by being lazy with their ID and password security), **and (b)** the same real or social identities (e.g. Names) associated with different people and accounts (e.g. Content from one get incorrectly associated with the other).

  1. **Digital Identity:** Of the many companies associated with ***'digital identity',*** most **offer either (a) 'Real Identity' (with social monitoring) protection services** (primarily monitoring credit reports; above), **or (b) people-search type services** (e.g. whitepages, reverse phone, email/address, background, criminal, public, genealogy, property, employee information), **that now incorporate looking up each person's social media postings, and (c) charge a fee** for extended search services, that often include **(i) restricting posted** content elements (e.g. Spokeo), **or (ii) claiming/ dis-claiming** association with content by the 'same name' or id (e.g. Providing resolution for problem 'b' above).

  2. **Reputation Management:** There is also a **third 'breed'** of companies (ex: Reputation.com, Brand.com, Integritydefenders.com @$100+/month), addressing negative social content, listed under ***'reputation management',*** **claiming to 'hide' or remove** published negative content on the Net (first search page). **Unfortunately, for the individual,** of the many tools listed under 'Reputation Tracking' tools, most are for businesses; only 'Reputation Defender' (at the time of this writing) offers services to track people's more personal social postings (at a reasonable cost), as compared with an 'individual' blogger (who is really a personal business)

IV. SMRC's *Preventative* Services - about early warning: monitoring & alerts; all topics; in-depth comparative profiling: By contrast, SMRC's services are designed to be preventative, filling in the missing searches that catch problems before they happen,***for real and social identity(s), scoping all topics in discussion, as compared to just purchases or bank accounts.*** For example, with identity fraud, before creating false financial accounts (to be 'bounced' later) using stolen identity information, it's typical to set up other Internet and/or physical 'accounts' (ex: memberships) using bits of the stolen identity, that create 2nd references that are used to further perpetrate the fraud. Knowing an in-depth profile of likes & dislikes, across all topics and covering all media that SMRC can access publicly, provides the best opportunity to uncover any potential harmful content that is 'out of profile'.

- **Social Identity Protection *Example*:** By monitoring for each person's social identity(s) in addition to their real identity elements, SMRC will identify any "spoofing" (hijacking) of a person's social identity. Before you think, "that's not important" or "that doesn't happen much", consider the 18 year old in Texas, who has been held without trial by the government (case: imminent threat) since February 2013 for a remark (from a movie) he made on Facebook, that ended with the Internet phrase "LOL JK" (laugh out loud, just kidding). For more on that story, see our press release link on the SMRC's home page.

- ***Advisory*: The most important security precautions related to identity** that each person should do now, in addition to**(a) putting a security freeze on your credit reports** (see more under 'security policies'), is to **(b) insure that their Facebook (TwitterYouTube, etc.) id and passwords are not the same** as they use for any sensitive information accounts - This is the **primary way** sensitive information is compromised today - because people are lazy about their security - and by that admission, fuel the largest industry in the world (one of the counterparts to identity theft - using stolen credit information to create more bad credit liability). By contrast, very little sensitive content is hacked from sites that carefully observe all known hacks. **For handling other 'identity problems', see #3 in the next section.**

- **SMRC Data Security Access Policies** - 1 way encryption & biometrics access:

  ⇨ **Processing Content (Enterprise Object database: File level access):** After each processing scan of authorized social content, a copy of the analyzed artifact (emotionally rated themes, social relations, philanthropy, location & demographics) stripped of any real or social identity content, is made available to SMRC. The user`s data is then encrypted with a one-way (hash) encryption, and rotating keys where the long passphrase is never shared (even with SMRC or the persona`s owner).

  Combined with biometric access security (next), this insures that the security to protect the analysis contents, is never compromised by anyone - **even from the owner attempting to give access to their best friend** - as that friend cannot replicate the owner`s biometrics.

- **Access to the analytics (search pattern apps: record level access)** - through the five (5) search pattern applications will be controlled through (a) one of multiple formats of **biometric security** (typing, audio, finger, eye & many more) and (b) **in-depth profiling** specific to each person - not as a static set of information that can be compromised but rather from a combination of (i) **long term** unrecognized behavior and (ii) **recent minor deviations** from a profiled pattern, where (c) the accuracy of the security method applied is **directly related** to the sensitivity of the content to be exposed.

  SMRC`s Founder was the marketing manager for one of the first U.S. software patents - *"The Electronic Signature Lock", funded by the National Sciences Foundation*, where the way a person types their own name (pressure, timing, inter-timing, emotion) is respectively unique (1 in 10 million), changes over time (e.g. is never identical) and **is linked *directly* to any, of each person`s individual biometric signature.** Advancements in directly related VSA applications over the last 30 years since that U.S. patent, now allow for precise **deviations of emotions distinguishing** between for example, extreme passion and fear, specific to each individual.

- **Handling Identity Problems:**

  - **Real Identity Fraud:** For financial fraud related to commerce (or false accounts anywhere that use stolen identity content), the best practice for such fraud, is the same as for any financial crime, that includes reporting the fraud (with evidence) to (a) the police, or the appropriate government enforcement agencies, (b) the major credit bureaus - see below, (c) your bank and the respective financial institution (or merchant or credit card company) related to the fraud case, (d) the management of the site with the fradulent material, and to (e) the Internet monitoring and reporting services (with any related tracking information that is different - e.g new email address, new address, alternate phone number, etc.).

    If you have reason to suspect a security breach, **you can place a 90-day fraud alert on your credit report** that warns lenders to be more vigilant about granting credit. **Consumer Reports says for added protection, place a security freeze on your credit report** so that lenders you don't already do business with, like banks, won't have access to it. That makes it more difficult for crooks to open new accounts in your name. But if you apply for new credit, be aware you'll need to temporarily lift the freeze, which could involve a small fee.

  - **Social Identity Fraud:** If someone manages to 'spoof' your social id (meaning they have the password associated with that id), you should (a) scan your system for viruses and/or malware first; This is how many hackers get in, (b) delete your cookies, making sure that you have any associated passwords that these cookies contain saved (or don't delete those cookies), c) Change your password in the associated media, and (d) use a secure option (e.g. https) to access that site, if that option is available. After that, you may have to do some 'damage control' regarding any content submitted by the spoofer (see below), as well as contact the site's administrators where your identity was compromised.

    While most anti-virus programs scan for some malware, **SMRC recommends the use of Spybot.** By contrast, the quick scans of Malwarebytes only catches a portion of the those items in startup (of the system or program initiations). Their startup analytics also allow for a quick review of startup and key executables of data gathering software (patterns).

  - **SPAM:** Many of the links that contain malicious code (which gathers identity content as compared to session content, e.g. your place in a process), are delivered through unsolicited spam email. Respectfully, a Gmail's secure (Https) web access (as a Gmail email address) and automatic spam filters provide a secure environment, without spam, on-line, as well though an email client like Outlook. If you are not using a Gmail email address, but want to leverage Gmail's spam filtering capability with your non-Gmail email address, you can have your current (non-Gmail) email address forward its' messages into a Gmail email account, which is afterwards forwarded back to your email client. Google the words "Gmail Extract Email Addresses Software" and use that software to extract the email addresses from your Gmail Spam folder, into (as an import) your Email client program (e.g. like Outlook).

    Alternately, you can export the email addresses in a Gmail spam folder by selecting up to 25 messages at a time in the Gmail spam folder, then selecting "more" "Filter Messages Like These", and then copy and paste the emails (separated by "OR") into notepad, editing out the "OR" statements, and ending each line with a carriage return - then import that file into your email client's spam filters.

- ⇨ **For Negative Content:** *Rather than respond to the invalid negative comment directly (e.g. By the accused), let your other friends and followers respond.* Similar to advertising where 70%+ of people today believe the word of 'trusted' third party strangers over the advertiser's claims, the response from your friends and followers is much more powerful than the individual responding in defense. Respectfully, if 10 friends respond negatively to a negative comment, **it turns that negative comment into a favorable one,** in defense of the negative comment (showing the world, that the negative comment was slander as compared to being true).

V. The *Effective* Cost of Identity Protection:

It seems like SMRC is "paying" (as donations +rewards) people for the opportunity to protect themselves, using their own content, where the more they participate, the better their protection gets (what a novel concept). With no out-of-pocket costs for members, SMRC's service costs are based on 8% of the SMRC total derived research value ($0.03, $1-2 & 5% units) for their content, research response (precisely matched), and networking activity (at set rates). From the 5 personalized search pattern applications, the majority of which are totally user-centric (Precisely Personal, Social simulations, Social World/Doppelganger & Identity), **the feedback from each continually adds value to (A) the identity search pattern** (#5 search, **growing in value daily**) and **(B) the sponsor match and qualify search pattern** (#4 search), that funds all the system`s content, research, commerce (post-purchase research), 501-c3 funding and charitable/deductible rewards - without requiring anybody purchase anything and never producing spam.

Author: Phillip R. Nakata, SMRC Founder & CBO; 720.569.7703; phillip.nakata@socialmarketresearchforcharity.org