Primary Psychiatry. 2010;17(8):29-31

Managing Your Digital Identity

John S. Luo, MD

Today, in this information era, all types of information are available for communication or exchange of ideas. The quick adoption of Web 2.0 technologies, such as Facebook and Twitter, has brought about a new paradigm of "share first and worry later." In particular, the younger generation of Internet users finds the connectivity of the Internet to be a powerful medium, creating a playground for a gregarious online persona of an otherwise shy teenager at school. Yet, all this access to information raises the question of how much information available online is too much, and is it really true, as Scott McNealy, former CEO of Sun Microsystems stated, that '"You have zero privacy anyway. Get over it." This column explores to what extent personal and professional information are found on the Internet and how to manage your "digital identity."

BACKGROUND

Technologies on the Internet have evolved and are implemented at a rapid pace, largely to be the first to stake out a new "space." Such pressures are understandable, as these companies strive to be innovators to create financial success and media recognition. In the early days of the Internet, its predecessor, the Advanced Research Projects Agency Network, was innovative with developing connectivity without the use of direct circuit connections.[1] Berners-Lee dramatically enhanced this information connectivity by developing a global hypertext project using HTML to communicate between Web-client and server, now known as the World Wide Web.[2] The plethora of Websites to visit created a vast resource of information that became increasingly challenging to navigate. Companies such as Yahoo[3] provided categories of Websites organized in hierarchies to facilitate finding the right information. Google[4] then took this process up a notch with a search engine that was capable of finding the relevant Website and information quickly and accurately.

Nowadays, using the search engine Google has become an integral part of our lexicon. The term "Google" is now synonymous with "search on the Internet," much as Kleenex has become the term used in reference to a popular brand of tissue. Finding information today has become an easy exercise by typing a few key words into the search engine box. However, the information found by most search engines today is located on traditional Websites, which are sites that contain information that changes little from day to day and are linked to other pages. More detailed and often desired information is located in the "deep Web," information that is often created dynamically as a result of a specific search.[5] These sites are often databases, shopping and auction sites, white and yellow pages, job sites, and message/chat forums. It is in the "deep Web" that much personal and professional information has become easily discovered without much effort compared to the traditional "surface Web."

DIGITAL INFORMATION

Numerous "deep Web" search engine sites have made such personal and professional information readily available to the inquiring mind or identity thief. Pipl,[6] 123people,[7] Peoplefinders,[8] PeekYou,[9] Spokeo,[10] Wink,[11] and ZabaSearch[12] are examples of these deep Web search engines that focus on all types of publicly available information about people. For example, a search using this author on the Pipl.com site shows information obtained from social networking sites such as LinkedIn and Plaxo, shopping sites such as Amazon, general Web searches, video searches on sites such as YouTube, publication databases such as Google Scholar and Scirus, and blog posts. Multiple profile pictures are also listed from a variety of Web site sources. A repeat search on 123People.com and Spokeo.com demonstrated the sites ability to find information such as age, occupation, hobbies, children, names of spouse and relatives, residence location, and home ownership.

Some information is displayed in its entirety up front, while the majority of detailed information such as exact home address or phone numbers requires a payment for one-time access or a subscription to the service. The accuracy of information varies from site to site, as the author's name is not unique in the state or city. Many of the people search sites also provide links to their partner sites that provide background check information or search of property records.

Dr. Luo is associate clinical professor in the Department of Psychiatry and Biobehavioral Sciences at the University of California in Los Angeles; past president of the American Association for Technology in Psychiatry (AATP) in New York City; and Gores Informatics Advocacy chair at the AATP.

Disclosure: Dr. Luo reports no affiliation with or financial interest in any organization that may pose a conflict of interest.

DISCUSSION

This easy availability of personal information evokes strong feelings about potential breaches of privacy and raises significant concerns. Primary care physicians often share information about their children and hobbies with their patients, largely in the context of establishing and maintaining a relationship with them. This level of personal intimacy often creates a stronger doctor-patient relationship as the patient feels that they "know" their physician, who likewise has personal knowledge of them. However, this personal information is revealed and discovered in the context of an interaction, with disclosure at the discretion of the patient or healthcare provider. It is generally understood in this situation that this information exchange is not for public disclosure and remains in the context of the doctor-patient relationship.

For psychiatrists and other mental health providers, disclosing personal information has much greater significance. As discussed previously in TechAdvisor,[13] patients with knowledge of their psychotherapist's personal information may impact the therapeutic relationship since transference may be compromised. In particular, patients with knowledge of the psychiatrist's hobbies or interests may create an ethical dilemma for the psychiatrist by giving a gift.[14] Depending on the circumstances, accepting a gift may be appropriate and ethical, such as in the case of termination due to the graduating resident-physician or the patient who has recovered and seeks to thank the provider with a small gift. However, patients armed with information discovered on the provider's Amazon wish list may purchase items that are either too personal or expensive, creating an ethical dilemma. Additionally, their motivation may be in question, such as an attempt to equalize the power dynamic in the relationship by demonstrating their ability to access information not previously disclosed.

Perhaps of more distressing concern to mental health providers is the possibility that a paranoid, manic, or personality disordered patient with access to personal information could do more harm than simply creating an ethical dilemma for the psychiatrist. Although the incidences of violence against psychiatrists are very rare, nonetheless, violence is always a possibility depending on the various risk factors such as erotomanic delusions, history of violence, and positive psychotic symptoms of a persecutory nature.[15] It is probably highly unlikely that a sufficiently paranoid or manic patient has the wherewithal and presence of mind to sift through the large amounts of information discovered in these people search engines in order to stalk or harass the psychiatrist and/or their family members at home, but nonetheless, it remains a disquieting possibility.

On the professional front, an identity thief who possesses sufficient professional and personal information could fraudulently write electronic prescriptions and post comments on various sites acting as the physician. In 2007, the bloggers at MedGadget demonstrated that they could "hack" into the Sermo.com medical professional networking site and create an account.[16] Since that time, Sermo has improved its verification mechanism; however, someone could ruin the reputation of a physician on the site by posting erroneous information or using rude behavior. The National E-Prescribing Initiative, in its authentication process, asks for some personal information such as the city name of a previous residence, in order to create an account.[17] An identity thief with the right information found on the Internet could create an account on behalf of the physician, and then write electronic prescriptions for controlled substances now that the Drug Enforcement Administration has revised regulations to permit these prescriptions to be electronic.[18] Fortunately, the authentication process for the National E-Prescribing Initiative requires answering at least five questions correctly, thereby significantly decreasing the likelihood that a thief could impersonate a physician.

COUNTER MEASURES

Despite the potential fear and anxiety generated by this column, there are simple and commonsense counter-measures to protect and manage one's digital identity. First, it is important to know what information is readily available to patients and thieves using these people search engines. Once the vulnerabilities are identified, it then makes sense to rectify them. For example, to manage what is displayed on the Amazon wish list, edit the profile and remove location, hobbies, and other interest information. Mark the ship-to address, birthday, and city to be available only to friends or private. Do not include a picture or caption, and check the profile of family members to ensure that their privacy has been set appropriately as well. In addition, some of the people search engine sites provide the option to have listings removed. While this may remove the aggregated information listing from the specific site, it does not remove information from third party sources.

Although this strategy may appear counterintuitive, another method is to create a listing or account on the people search site. By creating a profile, it provides a limited amount of control by designating what information is shown, such as office location and work phone numbers. This strategy is not necessarily appropriate for every people search site since they may collect information for distribution to their affiliates as a condition to create the account. Careful reading of the terms of service as well as privacy policy is of utmost importance prior to implementing this technique.

A number of companies provide "protection" by monitoring credit bureaus and Internet identity trading activity, removing personal information from online databases, and monitoring searches on the Web. These companies include LifeLock,[19] ReputationDefender,[20] and Identity Force.[21] Their services are available for a monthly or yearly fee, and may provide some peace of mind.

CONCLUSION

In today's information age, it has become increasingly difficult if not impossible to remain anonymous. Physicians generate information that can be shared on Websites and organizations create Web pages with physician information. Databases silently collect and aggregate data unbeknownst to users, who often forget that Web site cookies remember passwords and also what and where users have visited. Patients and family members create information online that contribute to one's digital identity. Even the location of computers online can be roughly determined by Websites that can trace back the IP address. However, despite the potential for misuse and abuse, access to information online is a fundamental benefit. By taking a few common sense precautions, safeguarding the digital identity may not be perfect but good enough until better procedures and services are established.[22] ***PP***

REFERENCES

1. Hauben M. History of ARPANET. Available at: www.dei.isep.ipp.pt/~acc/docs/arpa--1.html. Accessed July 8, 2010.
2. Biography of Tim Berners-Lee. Available at: www.w3.org/People/Berners-Lee/Longer.html. Accessed July 8, 2010.
3. Yahoo. Available at: www.yahoo.com. Accessed July 8, 2010.
4. Google. Available at: www.google.com. Accessed July 8, 2010.
5. Bergman MK. The Deep Web: Surfacing Hidden Value. Available at: http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104. Accessed July 8, 2010.
6. Pipl. Available at: www.pipl.com. Accessed July 8, 2010.
7. 123People. Available at: www.123people.com. Accessed July 8, 2010.
8. PeopleFinders. Available at: www.peoplefinders.com. Accessed July 8, 2010.
9. PeekYou. Available at: www.peekyou.com. Accessed July 8, 2010.
10. Spokeo. Available at: www.spokeo.com. Accessed July 8, 2010.
11. Wink. Available at: www.wink.com. Accessed July 8, 2010.
12. ZabaSearch. Available at: www.zabasearch.com. Accessed July 8, 2010.
13. Luo JS. The facebook phenomenon: boundaries and controversies. *Primary Psychiatry.* 2009;16(11):19-21.
14. The principles of medical ethics with annotations especially applicable to psychiatry. Available at: www.psych.org/MainMenu/PsychiatricPractice/Ethics/ResourcesStandards.aspx. Accessed July 8, 2010.
15. Rosack J. Patient charged with murder of schizophrenia expert. Available at: http://pn.psychiatryonline.org/content/41/19/1.1.full. Accessed July 8, 2010.
16. Medgadget's guide to hacking into social networks for doctors. Available at: www.medgadget.com/archives/2007/09/medgadget_guide_to_hacking_into_social_networks_for_doctors.html. Accessed July 8, 2010.
17. National e-prescribing patient safety initiative. Available at: www.nationalerx.com. Accessed July 8, 2010.
18. Electronic prescriptions for controlled substances. Available at: www.deadiversion.usdoj.gov/ecomm/e_rx/index.html. Accessed July 8, 2010.
19. LifeLock. Available at: www.lifelock.com. Accessed July 8, 2010.
20. Reputation defender. Available at: www.reputationdefender.com. Accessed July 8, 2010.
21. Identity force. Available at: www.identityforce.com. Accessed July 8, 2010.
22. Safeguarding digital identity. Available at: www.thei3p.org/research/safeguarding_identity.html. Accessed July 8, 2010.

