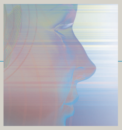

BY GREGORY CONTI

COULD GOOGLING TAKE DOWN A PRESIDENT?

Everything we do online is known and knowable and can be combined with everything else that is known and knowable.

In the August 1984 *Communications,* Ken Thompson taught us to question our notion of trust, recognizing that even our most carefully crafted code might not generate trustworthy executable programs if the compiler is compromised [5]. Looking to the future, however, I realize Thompson didn't go far enough. Today, we must question our trust in all aspects of the information environment, including online companies and even the infrastructure of the Internet. We live in an era of rampant data disclosure and ubiquitous implied trust—two factors that will come to haunt us in the near future.

We disclose sensitive and ultimately personally identifiable information to our Internet service providers (ISPs) and favorite online organizations of every type and purpose each time we sit down at the computer. Don't believe me? Imagine if Google, Yahoo, or MSN aggregated and mined every search query emanating from your corporate IP space and every email containing your corporate domain name. Strategic plans, blackmailable material, health concerns, and social networks would all emerge. We are placing unprecedented power in the hands of the most popular online companies and ISPs, along with thousands of others, and there will come a time when it will be difficult or impossible to wrest back that power.

Could Googling take down a president, prime minister, congressman, or senator? The question is provocative but worth considering as we face the near future of trust and privacy. Googling[1] is an integral

[1] By Googling I mean the full spectrum of free online tools and services (such as search, mapping, email, Web-based word processing and calendaring).

part of the Internet fabric. Approximately one billion Internet users worldwide rely on networked technology to provide information and interconnection for all aspects of their lives, both personal and professional. Everything from our physical location, to what we think, to who we know can all be found in this data. Despite the best intentions of those doing the collecting or communicating, it is impossible to guarantee it will stay private or not be used for some malicious purpose. As an example, AOL disclosed, in August 2006, the search queries of some 657,000 of its users that contained sensitive and personally identifying information [1]. This incident only hints at the risks the world's most powerful leaders, as well as ordinary citizens, face when using myriad "free" tools (such as search, email, mapping, news, word processing, calendaring, and blog hosting). Free online services aren't really free; we pay for them with micropayments in the form of personal information [3].

One billion users, while a very large number, represents less than 18% of the global population and just a fraction of those who will turn to the Internet in the future. Although some progress has been made, these most sensitive of our hopes, dreams, and intentions [2] are routinely passed to online companies that scrupulously log and retain our revelations, sometimes indefinitely, where they are data-mined to allow customized advertising and help improve our online experience. Encryption offers little help, as online companies are a trusted party in the communication. Your computer and its Internet connections accelerate the loss of privacy. Counterintuitively, the more usable a given online application, the worse it is in terms of our personal privacy. Online companies are not the only ones with access to this information. It also flows across the networks of our ISPs, which have the power to collect, and even alter, practically every bit we send and receive. The information visible to online companies and the ISPs is largely the same; only the network vantage point is different.

In most instances of online navigation and interaction, it would be prudent to assume that these disclosures are never discarded. Once a disclosure is made, it can never be undone. At best, we must trust our ISPs and online organizations to eventually discard the information. At the same time, network neutrality is under attack. We cannot assume the information we receive is what the information provider actually sent.

In some ways, trust is increasingly irrelevant, because, if we are to be members of the Internet-enabled society, we have no other option but to rely on the powerful tools we have at our disposal (such as those provided by major search engines). Like rats forced to endure electric shocks to acquire food, we must use these tools to acquire information and communicate. The implications of data disclosure and retention are profound, including corporate and law-enforcement abuses and identity theft, as well as second- and third-order effects impossible to predict. Those of us who are aware of the risks already self-censor our activities, even as we continue to indulge them.

Those of us who are aware of the risks already self-censor our activities, even as we continue to indulge them.

What is most worrisome is less that the data is being collected at any given moment and more how it will be used (and abused) in the future. Future advances in data mining, profiling, and machine learning are particularly worrisome. While I don't foresee a dystopia in the near future, I do see a steady decline in individual freedoms and civil liberties. This decline is not new, dating back to at least the 1970s when large computerized databases of personal information were being formed in earnest. The pace accelerated globally in the aftermath of 9/11. Will we eventually reach equilibrium? I think not. The gravitational pull of both profit and power will continue to drive the decline.

Public outcry may have the power to stem the tide, but public opinion is fickle. Even the 2005 Sony rootkit incident, in which tainted Sony CDs were able to infect hundreds of thousands of end-user PCs, and the 2006 AOL data spill did little to penetrate the public consciousness. In one 2007 study only 16% of the participants reported being familiar with the AOL incident six months after it took place [4]. If this lack of public interest characterizes the general population, a less extreme rate of change will be unable to generate enough resistance to make a difference.

People have only a small window of experience to use as a reference. Chances are you lived through 9/11 and knew adult life before that day. You have a reference point, but when our generation is gone, few guides will be available to show how to defend our personal privacy. Those in power are loathe to relinquish or even share it. And, as the power and control this information (and its data-mined results) provides over hundreds of millions of citizens is seductive, corruption is inevitable. Action is critical, before it is too late to forestall individuals from losing control of their own data and perhaps even of their digital identities.

I don't want to live my life inside a Faraday cage and abandon the Internet. To do so would force me to withdraw from modern society. The future I foresee isn't guaranteed; each of us has the innate ability to influence the trajectory of technology development and use. The public is unaware, apathetic, or sees no other option than the status quo. But each of us is able to change it. As the world's leading technologists, we have the power to seek and find equitable solutions that would protect our privacy, increase our trust, and still allow online businesses, social interaction, and network providers to innovate and flourish.

In the future, Googling could indeed take down a president, yield a cure for cancer, and ruin or enrich our lives. We have to live with the past decade's worth of disclosures, but promising solutions are on the horizon. Whether they include paying for privacy, better tools for self-monitoring online activity, anonymous browsing, informed law-making, privacy-protecting corporate policy, increased user awareness, or something yet to be discovered, the solution is up to each of us.

References

1. Barbaro, M. and Zeller, T. A face is exposed for AOL searcher no. 4417749. *The New York Times* (Aug, 9, 2006); www.nytimes.com/2006/08/09/technology/09aol.html?ex=1312776000en=f6f61949c6da4d38ei=5090.
2. Battelle, J. The database of intentions. John Battelle's Searchblog (Nov. 13, 2003); battellemedia.com/archives/000063.php.
3. Conti, G. Googling considered harmful. In *Proceedings of the New Security Paradigms Workshop* (Schloss Dagstuhl, Germany, Sept. 19–22). ACM Press, New York, 2006, 67–76.
4. Conti, G. and Sobiesk, E. An honest man has nothing to fear: User perceptions on Web-based information disclosure. In *Proceedings of the Symposium on Usable Privacy and Security* (Pittsburgh, July 18–20). ACM Press, New York, 2007, 112–121.
5. Thompson, K. Reflections on trusting trust. *Commun. ACM 27,* 8 (Aug. 1984), 761–763.

Gregory Conti (conti@acm.org) is Director of the Information Technology and Operations Center and an Academy Professor of Computer Science at the United States Military Academy, West Point, NY.

The views expressed here are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the U.S. Government.