



Online Exposure, Offline Uncertainty:
Privacy and Security in a Virtual World

October 2009

INTRODUCTION

By almost any measure, the advent of the Internet has revolutionized the way America lives, putting unprecedented power and knowledge at the hands of tens of millions of individuals in this nation alone. From commerce to communication, this new information age has brought progress to virtually every corner of society. Yet it has also left millions of Americans increasingly anxious and even fearful about its costs and consequences.

One such consequence is the threat posed to the security of their personal information online. Americans are generally aware that any online activity has the potential to expose their personal data to exploitation, but few understand the different risks posed by different actions, or how vulnerable their online identities may already be. Most are especially concerned about active as opposed to accidental misuse of data, including the theft not only of information but of identity. Driven by these concerns, and skeptical that there are answers on the horizon, Americans are increasingly reluctant to participate in further technological advances and the progress they help fuel.

These concerns are hardly ill-founded; incidents of online data misuse and identity theft are increasing significantly each year. This general anxiety is compounded by the fact that most Americans, while broadly aware of the dangers posed by an online existence, fail to recognize how these risks translate to our everyday lives. Most Americans, for example, remain unaware of our widespread exposure to the cloud – through web-based e-mail like Yahoo or Gmail, for example – and the new vulnerabilities the cloud creates. In addition, Americans feel little empowerment when it comes to protecting themselves online; they typically fail to take even the most fundamental steps to reduce or manage their risk and protect their cyberspace selves.

The challenges and opportunities confronting Americans online were studied in a phone survey of 1,003 Americans conducted on August 6 – 13, 2009 by Penn, Schoen & Berland Associates (PSB) in conjunction with the Chertoff Group. The margin of error is plus/minus 3.1% and the sample was balanced by geography and demographics. This paper will highlight and analyze some of the key findings and implications of that survey.

As more and more of the world's business moves to the Internet, the need to respond to the problems and perceptions of online data and identity vulnerability continues to grow. These findings underscore the need for individuals and organizations to do so in a deliberate, constructive, and methodical way. They highlight the imperative of strengthening Internet security today, so we can ensure continued technological and material progress tomorrow.

CONCERN ABOUT ONLINE SECURITY & MISTRUST IN INSTITUTIONS

The overwhelming majority of survey respondents -- 81% of those responding -- expressed concern about the security of their online personal information. Moreover, 54% of respondents said they were "very concerned" about their personal data sent over the Internet.

This remarkably high level of unease is shared almost equally by both genders and by every age group under 65. Seventy-nine percent of males and 83% of females were either "very concerned" or "somewhat concerned" about what can happen to their online information. Similarly, 85% of respondents under age 35, 84% in the 35-49-year-old age bracket, and 80% of those between age 50 and 64 said they were concerned.

For Americans 65 years of age or older, the figure declines markedly to 69%. Although this is still a significant percentage, the divergence of the over-65s from the under-35s is a key finding throughout the survey.

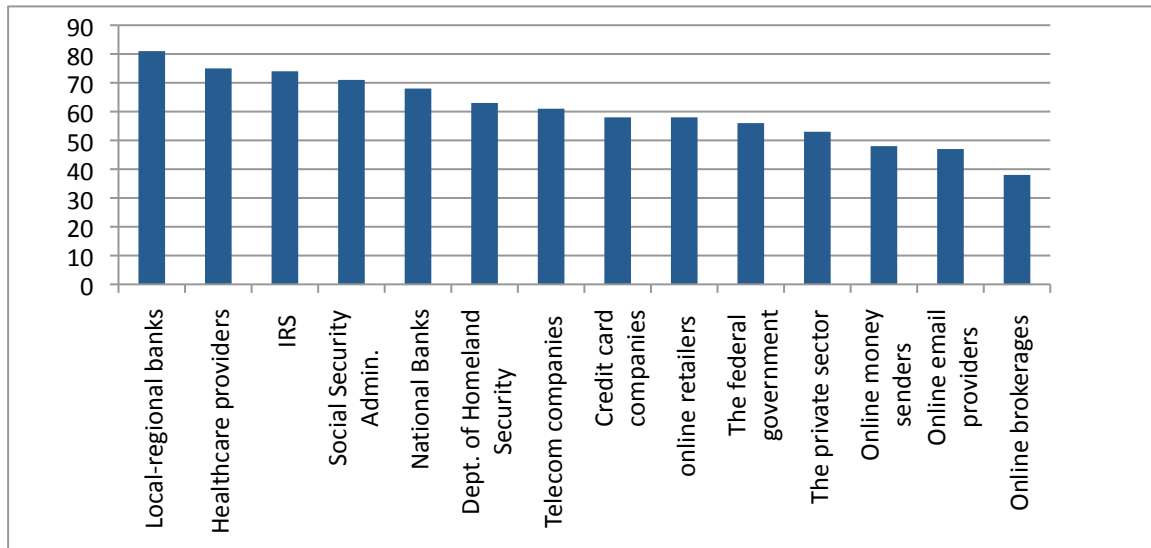
This inter-generational distinction could reflect a correlation between level of exposure or familiarity and level of concern. Senior citizens may be less worried about their vulnerability because they are not as familiar with the risks of the Internet or simply spend less time in cyberspace.

Which aspect of online vulnerability most concerns Americans? By far the greatest fear of the respondents was that of identity theft. Members of every age bracket cited it as their primary online-security concern, followed by the malevolent hacking of personal data.

Tellingly, these and other primary concerns center on active as opposed to accidental incidents. Americans are far less focused on the equally grave risk of security issues triggered by honest errors or mistakes arising in the natural course of cyberspace activity.

Which institutions do Americans most trust to keep their online information secure? Based on the survey results, respondents tend to trust tangible offline institutions such as local or regional banks and healthcare providers the most, and online-only establishments such as e-mail providers and online brokerages the least. They also have higher levels of trust for specific organizations like the Internal Revenue Service and the Social Security Administration than for general institutions like the federal government or the private sector.

How much confidence do you have in the following organizations to keep your information secure?

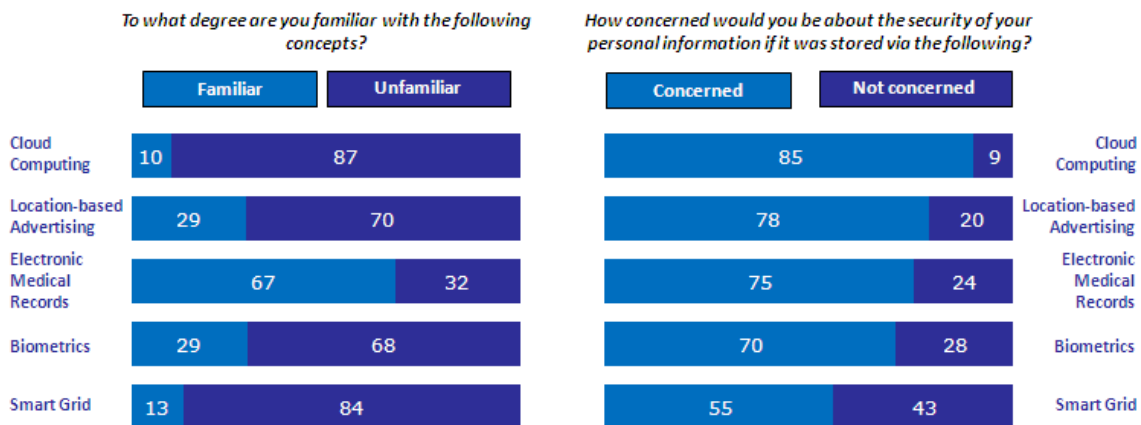


As in the overall assessment of online security, degrees of trust break along age lines. Respondents under 35 years of age tend to have greater trust in the federal government, while older Americans, particularly over-65s, have more faith in private institutions and companies. Overall, however, only one in three respondents expressed a great deal of confidence in even the highest rated entities in the survey.

UNFAMILIARITY WITH NEW TECHNOLOGIES ONLINE

While Americans clearly have a high level of general anxiety about online security – coupled with a low level of confidence in the ability of even the most trusted organizations to safeguard their personal information – they also share a deep concern about the security implications of new technologies with which they are largely unfamiliar.

Thus, 87% of respondents were unfamiliar with cloud computing and 85% would be concerned about the security of personal information if stored in the cloud. Seventy percent were unfamiliar with location-based advertising, while 78% of respondents worried about the security of their personal data if used for such an application. Sixty-eight percent were not familiar with biometrics; 70% of them would be concerned about the security of personal information if stored for use in biometric identification



One of the most significant revelations in the poll findings is how many Americans are already exposed to these technologies without realizing it. While 87% of respondents surveyed believe they have never used cloud computing services, 65% report using these services in the form of web-based e-mail; in short, they are in the cloud without even realizing it. Similarly, while 70% of respondents claimed zero familiarity with location-based advertising, 41% said they have received online advertisements that reference their approximate geographic location

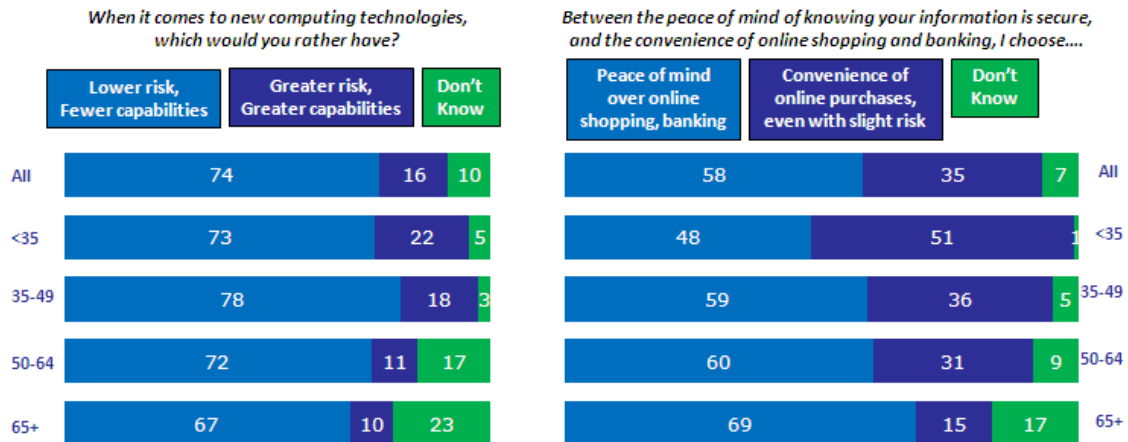
Since Americans are generally unaware of this exposure, they are by and large failing to take any kind of protective measures such as regularly changing their passwords. Although Microsoft, for instance, recommends that IT departments mandate that users change their passwords every 30 to 90 days, the average American has 3.86 passwords, and changes them just 2.5 times per year.¹ The ironic result of this ignorance is that Americans are neglecting to take even the simplest, most fundamental steps to protect themselves against the very things that concern them so profoundly.

VALUING SECURITY & PRIVACY OVER POWER & EFFICIENCY

Clearly, Americans have deep misgivings about online security, a profound lack of confidence in the ability of institutions and organizations to keep personal data safe, and a serious blind spot about their own interactions with new technologies which demand more vigilant security practices of their own.

¹ [http://technet.microsoft.com/en-us/library/cc784090\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc784090(WS.10).aspx)

Given these facts, it is not surprising that the vast majority of Americans are willing to consider what amounts to a strategic retreat from the battle for greater technology and progress. By an overwhelming majority, they prefer lower-risk computing technologies with fewer capabilities over more powerful and capable technologies that could present greater security and privacy risks. Nearly three out of four Americans -- 74% of survey respondents -- express this preference. This includes sizable majorities within every age group; 73% of Americans under the age of 35, 78% of the 35-49 age range, 72% of those between ages 50 and 64, and 67% of Americans who are 65 or older.



A majority of Americans – 58% of respondents -- are even willing to forgo the convenience of online shopping and banking for the sake of knowing their personal information is safe. This is true across every age group, except for Americans under 35. For these youngest Americans, there is a real split: 48% are willing to trade away the efficiency of online transactions for the promise of greater data security and privacy while the remainder are unsure.

These particular findings have obvious implications for the future of technology companies, especially those whose focus had been on cutting-edge innovation. Additionally, they also have implications for the future of our society. If security – or the appearance of it – begins to trump innovation for the American consumer, it could markedly slow the rate of technological change and the progress that comes with it. Clearly, it is in society’s best interests to find ways to enhance the security of existing online technologies before consumer fears harden into settled biases.

CONCLUSION

Americans are clearly worried about online security; while they are full and willing participants in the computer and Internet revolutions, reaping their rewards in numerous ways, they also perceive the potential dangers, especially those involving data and identity theft.

Given those risks, Americans have little confidence in the capacity of our society's institutions – especially online organizations -- to keep their information and identities safe. Additionally, most Americans fail to appreciate the vulnerabilities they're already exposed to online, and thus fail to take the necessary precautions to manage or reduce the risks they pose.

Believing that neither they nor any organization can successfully manage these dangers, Americans are prone to the fatalistic conclusion that the way to reduce risk is to retreat from continued technological advances.

This, in short, is the challenging landscape that confronts anyone doing business online, (in other words, everyone.)

It is a moment of anxiety and opportunity. There is a widespread crisis of confidence in the ability of our society to protect data and identity without scaling back on the use of the latest technology. There is also, however, an opportunity to confront this assumption by challenging both the consumer and the organizations that operate online.

Since the Internet revolution is not going away, there is an urgent need for consumers and other online users to do their part to reduce their vulnerability to data or identity crimes. One aspect of this is pushing users to act upon what they already know – the need, for example, to be wary of attachments from unknown sources and to change passwords regularly. Another is urging Americans to further educate themselves about what they don't yet understand, including their exposure to the latest technologies and the security implications that come with it.

Equally important, for the sake of their enterprises and continued technological advancement, it is time for online businesses and other organizations to confront the challenge by mounting a two-pronged response.

First, they must fully embrace and invest in the kind of technological innovations that can directly enhance security. Second, they must learn to communicate to a worried public what it is that they are doing. Innovation without communication will not restore the confidence in online institutions and businesses currently absent among Internet users.

Clearly, the future will belong to those companies and organizations that will take up both the security and the communications challenge. Firms that make it their priority to provide reliable, effective, and understandable security measures will survive and thrive in the coming years and decades. They will inspire trust and confidence in their consumers, establishing powerful relationships that will stand the test of time. In so doing, they will strengthen our society and help fuel progress for the next generation.

###

For more information, please contact:

Beth Lester
blester@ps-b.com
(202)962-3042

Russ Knocke
russ.knocke@chertoffgroup.com
(202)262-4976

About Penn, Schoen & Berland Associates

Penn, Schoen & Berland Associates, a unit of the WPP group (NASDAQ =WPPGY) is a global research-based consultancy that specializes in messaging and communications strategy for blue-chip political, corporate and entertainment clients. We have over 30 years of experience in leveraging unique insights about consumer opinion to provide clients with a competitive advantage - what we call Winning Knowledge™. PSB executes polling and message testing services for Fortune 100 corporations and has helped elect more than 30 presidents and prime ministers around the world. More information is available at www.psbresearch.com.

About The Chertoff Group

The Chertoff Group is a global security and risk management advisory firm that assists corporate and government clients in addressing threats related to terrorism, fraud, cyber security, border protection, and supply chain security. The firm is headed by former U.S. Secretary of Homeland Security Michael Chertoff and is based in Washington, D.C., with offices in New York. More information is available at www.chertoffgroup.com.