Testimony to the House Committee on Financial Services
Examining the Security Implications of Proposed Online Gambling Regulation

Jeff Schmidt
CEO, Authis
Friday, June 08, 2007

Chairman Frank, Ranking Member Bachus, and members of the Committee:

Thank you for the opportunity to speak to you today. My name is Jeff Schmidt and I am the Chief Executive Officer of Authis, a provider of identity and security-related products and services to the financial industry. I am a recognized expert on issues related to online identification and authentication, and have published numerous books, articles, and papers on information security related topics. I am also a founder, former Director, and current Officer of the InfraGard National Members Alliance, the private sector component of the FBI's InfraGard Program

My most recent scholarly article entitled *Online Child Safety: A Security Professional's Take*, discusses the issues of Internet-scale identification, authentication, and age verification. It was published in the Spring edition of The Gardian, the InfraGard National Members Alliance's peer-reviewed security journal.

I speak only for myself today and not for any of the organizations with which I am affiliated or for any colleague.

In my testimony today I would like to focus on two topics integral to the proposed legislation: the notion of "age verification" of persons remotely over The Internet, and the ability to determine the geographic location of an individual using The Internet.

Mr. Chairman, it is critical to understand that age verification and determination of geographical location simply cannot be done reliably over The Internet. As no security measure is infallible, good security practitioners always consider a-priori what happens in the inevitable situations when security measures fail. I appear here today to discuss the factors that contribute to the unreliability of these particular security measures. The facts are that these two particular security measures are inherently unreliable, can be trivially circumvented, and will fail at high rates. This reality must be taken into account when considering this proposed legislation.

Age Verification Is Not Reliable

Authentication is the difficult problem of verifying that persons are who they claim to be. Authentication is hard, expensive, and requires a delicate balance between cost, security and usability. Today, mass consumer Internet authentication is problematic: security is weak and irritated users are forced to maintain long lists of usernames and passwords. I would ask the distinguished Committee Members: how many usernames and passwords do you have?

At the root of nearly all “information age” security problems is the inability to reliably authenticate users (and computers) over The Internet. Identity Theft/Fraud, Phishing/Pharming, and even SPAM are all authentication problems at their root.

Authentication comes in many shapes and sizes. Some authentication techniques, such as photographs, physical descriptions, and secret handshakes, are only useful in-person. Moreover, some do a better job than others - we call this authentication strength. For example, when online, a simple username/password provides very weak authentication, while Smart Cards, tokens, or biometric measures provide a much stronger authentication. Reliable authentication at Internet scale is particularly problematic.

Academically, “age verification” is the act of attaching an attribute “age” (or “date of birth”) to an identifier. In other words, we attach an age (“45”) to an identifier (“Joe”). Once we’ve made that association, if we successfully identify and authenticate Joe, we’ll also know his age. We need the age information to be highly resistant to forgery, and we need authentication strong enough to make it sufficiently difficult for motivated persons to impersonate others.

“Age Verification” must be split into two separate problems I call the Initial Subscription Problem and the Subsequent Visit Problem. The first time (initial subscription) we see a person identifying himself as “Joe” how do we determine his age? In other words, how do we reliably associate the correct “age” attribute with this person? Then, on subsequent visits, how do we reliably identify and authenticate that the person claiming to be “Joe” is the same one we subscribed?

When attempting to age verify adults online, the Initial Subscription can be reasonably performed in many cases with public records. However, the security of the Subsequent Visits, authenticated only by a password, is in doubt: reliably matching the age verified identity to some person thousands of miles away on the Internet is fraught with peril. Again, this is the root of the “Identity Theft/Fraud” problem we face today in nearly all aspects of online commerce.

We know from experience that usernames and passwords are unreliable for Internet scale authentication. We also know from experience that clever and motivated minors will always find ways to circumvent any age verification system – from impersonating parents and siblings to sharing or stealing age verified identities. We also know that criminals harvest, use, and resell usernames and passwords.

Underscoring the fundamental problems with age verification at Internet scale, the attorneys general of 21 states recently lashed out at Anheuser-Bush’s Bud.tv age verification method, claiming it does little to keep minors from accessing the site.

When considering the proposed legislation, it is critical to consider that Internet age verification can not be done reliably and as such one must conclude that motivated minors will in fact easily and regularly circumvent the system.

Determination of Geographic Location of an Internet User Is Not Reliable

The Internet is a massive conglomeration of interconnected networks. Engineered by the DoD during the Cold War, a primary design goal was multi-path redundancy such that point to point communications could be maintained even if parts of the network were destroyed. These requirements lead to a highly decentralized network with literally an infinite number of paths between any two distant points. It is impossible to know in advance which path "through The Internet" traffic may take – and the actual path often changes transparently mid-communication due to numerous factors.

Internet Protocol (IP) addresses, like phone numbers, identify devices in the network. However, unlike the telephone system, most users connect to the Internet using dynamic IP addresses – a different address is transparently issued to their computer on each use and re-issued to others when communication ceases.

Moreover, the Internet is awash with technical measures including overt and transparent proxies, firewalls, filters and filtering services, Network Address Translators, private address spaces, point-to-point links, tunnels, and Virtual Private Networks (VPNs) which further obfuscate the true source and destination of communications. These technical measures are widely deployed and critical for the proper operation of The Internet.

For engineering reasons, Internet Service Providers (ISPs) often maintain large pools of IP addresses which are issued dynamically according to demand and technical factors. The same IP address may at one moment be in use by a user in Texas and then a moment later be assigned to a user in Ohio. The current explosion of wireless technologies including commercial and private Wi-Fi "hotspots" and "Mobile Broadband" technology (high speed Internet connectivity through the wireless cellular system) has greatly impacted the methodology carriers use to assign IP addresses even further detracting from the ability to reliably ascertain geographic location.

Additionally, users can very easily use various tactics including "anonymizers", proxies, and zombies to conceal or impersonate their location. In most cases, the use of these measures violates no law.

Based on all of these facts and absent supplemental data from a location-specific technology such as The Global Positioning System (GPS), reliable determination of the geographic location of individuals/devices on The Internet is simply not possible. While several vendors have built databases which attempt to match individual IP addresses to geographic locations, this data is most reliable at a "macro" level (i.e. identifying the country of origin) and not generally reliable at a fine-grained jurisdictional level. Data contained within these databases is highly dynamic and often inaccurate, lacks the granularity required to reliably identify jurisdictions, and can be misdirected both by technical measures inherent in the networks and by motivated users wishing to conceal or impersonate their location.

When considering the proposed legislation, it is critical to consider that physical geographic location of an Internet user can not be done reliably.