EDITORIAL PREFACE

Consumer Apathy and the Emerging Revenue Model of the Internet: The Economic Case for Spyware

Tom Stafford, University of Memphis, USA

Introduction

Since its early days, consumers have been socialized to expect the Internet for free. Of course, there has been a constant expectation that getting *connected* costs something; this is the basis of the Internet Service business, led by companies such as AOL and Microsoft Network. Yet, with the assurance of connectivity assumed as given, there seems to be the generalized expectation among users that most of the content and functionality online are "free." Most Web pages are free sources of valuable news and information, many software downloads, drivers, patches, and updates are available online without monetary cost — and, legal or not, music just wants to be free. Right?

That's how it may seem, even to those of us with sophistication in the matter. Even so, the old truism about lunch and freedom pertains equally well in the world of information as it did in markets of previous eras. The fact remains that mounting a respectable Web presence is not a cheap endeavor, and anyone who cares to do it ought to have a sure source of income derived from the subsequent online operation, or be prepared to operate the service as a general good and charity. This economic challenge is the crux of what is surely the most potent new security threat in computing: spyware.

A technical definition of spyware would be any application that, without user knowledge and/or permission, uses a computer's Internet "back channel" to communicate with an external server, while the popular press view is that any application that tracks user behavior without their knowledge and consent is spyware, regardless of its specific intent or legality (Stafford & Urbaczewski, 2004). The Federal Trade Commission, which probably carries the most potent regulatory authority to control spyware, defines it as software that aids in gathering information about a person or organization without their knowledge, and that may send that information to another entity without user consent (Urbach & Kibel, 2004).

Spyware is designed to monitor computers; the economic reasons for its existence have to do with all of the great freebies we find online. We should give careful thought to the economic tradeoffs entailed in providing online market offerings of putatively "free" goods and services, as a general business issue.

Software: Free Downloads Cost Money to Develop

Here's the business development challenge in the online applications marketplace: how do you get somebody to try something radically new and potentially illegal and risky, such as, say, KaZaA or Morpheus peer-to-peer file sharing applications? What reason would anybody have to pay money for a little cosmetic cursor utility chases your mouse pointer around the screen with a whirly "tail," or who would pay for yet another toolbar search utility when Google is already free, anyway? Notable examples of popular downloadable applications that carry spyware with them include Bonzi Buddy, Comet Cursor, and Gator (Coggrave, 2003), as well as Xupiter Toolbar, Bargains.exe and a host of peer-to-peer applications that proliferated for music and video file sharing (Taylor, 2002). These are all applications that can't really survive on their own; they need an economic symbiote.

Nobody would pay for them; why should they? There's lots more good free stuff online, just a Google search away, and just about the only thing in the way of online content that draws reliable and regular monetary payments is not something one discusses in polite company. That nifty little cursor chaser we all want to download for free costs money to develop, and free is not a lot of margin from which to pay down operational investments in software development.

Enter spyware. In the regulatory circles, it's well known that spyware providers pay other developers of recreational software to be included in their installation package (which is typically distributed for free or so cheaply that there's no real money in it, anyway). The spyware provider pays the legitimate developer a good deal of money to bundle their spyware applications in with sought-after downloadable applications and this economic symbiosis serves as the economic basis of survival for "free" application developers (Klang, 2003; Townsend, 2003). It's a clever economic arrangement: a company produces really nice applications, but due to the challenges of frictionless markets, can not make much money on them. Another company makes remote monitoring software designed to mine personal information for business gains, or even less legitimate purposes, but has no effective way to lure users into installing it on their computers.

Solution? Put your spyware application into the file-sharing download, so that the desirable P2P application serves as the vector for the spyware installation. Everybody profits. The P2P utility developer, without a revenue model in its early days, gets enough money to stay afloat. Spyware producers get handy access to millions of downloads, fueled by the frantic efforts of computer users to get the latest method for "free" music downloads installed on their computer.

No problem. It's all FREE, don't you know?

Not…

Spyware is a Security Threat

Spyware carries a cost. In what is surely emerging as the classic barter transaction of the online economy, computer users get software in exchange for personal information. File sharing software is free to download and install, but you [often unknowingly] agree to let some other third party monitor your computer in exchange for the freedom of MP3 file sharing at no discernable cost.

It's not expensive in monetary cost for a computer user to let someone else see what Web sites they view, or what key strokes they enter. But, it's not exactly cheap in real economic terms, either. SPAM inevitably ensues. Computer security is com-

promised. Who knows who *really* gets to look at your computer once the monitoring software is installed? The compiled personal information profiles of large groups of users is a very valuable target marketing commodity.

Ain't No Free

I have taken to presuming that anything I do online is monitored. One's employer, we assure our students, most certainly monitors employee Internet use. Parents have ISP-provided tools to monitor their children. Spouses monitor each other. Everybody's looking at something, online, and usually it's something personal, it seems like. You just have to develop calluses on your privacy expectations. That, or be willing to pay what fabulous P2P apps really cost to develop; any good software application is never really cheap or truly free.

Consider Kodak. Now, Kodak has digital cameras, and these require software to operate. Naturally, one wishes to update software to be competitive with all the other digital camera companies out there, in terms of features and functionality. What to do if you're Kodak, and have [famously] outsourced your IT function? You need an update agent, and you don't have a dedicated development staff, anymore. Should you pay market rates for a solution? Or, could you use an off-the-shelf remote monitoring application to "make do," on the cheap? Sure, it's cheaper to make do. The solution is called BackWeb lite, and in my experience on a Sony Vaio computer, it monopolized CPU cycles and ISP bandwidth when I had the Kodak imaging software installed; clearly an unintended consequence, but what to do, all the same? Cleaning the BackWeb-supplied Kodak software update agent with Spybot Search and Destroy identified at least 59 registry entries made by the monitoring software. Seriously, my camera is pretty basic, I don't think it really needed that much updating.

Consumer Apathy in the Face of Shock and Awe Security Threats

Spyware is just about everywhere. You get it by looking at Web sites, it comes in software downloads, you even get it in OEM installations, go figure (Levine, 2004; Thompson, 2003). What is surprising to me is that consumers are not really willing to do anything about it. This is just what I found in my recent study with AOL. Sure, AOL members know about spyware, it's right up there with viruses in terms of recognition as a threat. But how much will they pay to do something about it? Not much, nada, zip, zero.

I exaggerate. They aren't really eager to pay for spyware protection, but they do like the idea and will happily take it if it is free, which motivates an economic model of threat protection upgrades just for general goodwill on the part of service providers like AOL or security protection providers like Symantec or McAfee. And you have to wonder what's in it for *them*, writing all that extra code. Sort of reminds you of the old KaZaA/Gator barter deal…

Seriously — I don't think people are cheap regarding good computer security. Norton AV costs more just about every time I renew it, and I continue to do so happily, it's fine protection, I'll gladly recommend it to you. Yes; folks take steps to protect themselves, but with regard to spyware, it's just so prevalent, one may simply be numb to the threat. After all, spyware is just a few more pop-up ads, and, gosh, would we even notice a slight increase in our SPAM levels, already at historical levels?

The Need for Understanding

Little empirical work exists to establish the prevalence and magnitude of the spyware

problem (Beales, 2004). As the outgoing chairman of the FTC bureau responsible for spyware regulation noted, we really ought to be taking a close look at this new economic symbioses. It forms the basis for a new economic model for online business, the consequences of which we might not be willing to accept once it is fully entrenched in the market.

References

Levine, J.R. (2004). Written comments of Dr. John R. Levine. U.S. Senate Committee on Commerce, Science and Transportation. Retrieved July 14, 2004, from *http://commerce.senate.gov/pdf/levine032304.pdf*

Beales, J.H. (2004). Remarks of J. Howard Beales, Director, Bureau of Consumer Protection. *FTC Spyware Workshop,* April 19. Retrieved July 20, 2004, from *http://www.ftc.gov/bcp/workshops/spyware/index.htm*

Coggrave, F. (2003). How to tackle the Spyware threat. *Computer Weekly,* November 18, p. 30.

Klang, M. (2003). Spyware: Paying for software with our privacy. *International Review of Law,Computers & Technology, 3*(17), 313-322.

Stafford, T.F., & Urbaczewski, A. (2004). Spyware: The ghost in the machine. *Communications of the Association for Information Systems, 14,* 291-306.

Taylor, C. (2002). What spies beneath. *Time, 15*(160), p. 106.

Thompson, R. (2003). Cybersecurity & consumer data: What's at risk for the consumer? Testimony before the U.S. House of Representatives Subcommittee on Commerce, Trade, and Consumer Protection. Retrieved from *http://www.iwar.org*

Urbach, R.R., & Kibel, G.A. (2004). Adware/Spyware: An update regarding pending litigation and legislation. *Intellectual Property & Technology Law Journal, 7*(16), 12-16.