The Changing Internet: Hips Don't Lie

Remarks of Commissioner Jon Leibowitz[1]
at "Protecting Consumers in the Next Tech-ade" Hearing
November 6, 2006

It is hard to predict the future, and even the brightest people don't always get it right. Take Woody Allen. In his 1973 film ***Sleeper***, he played a health food restaurant owner who is cryogenically frozen and defrosted centuries later. In Allen's vision of the future, scientists have learned that cream pie and hot fudge are actually ***good*** for you. Of course, we'll have higher expectations about our experts' predictions today.

This is the second time that the Commission has gathered the best and brightest to tell us where the Web is going – in 1995, the Agency held similar hearings. The Commission's report was surprisingly prescient. It warned that, unless controlled, "spamming" practices could hinder the healthy growth of the Internet. It pointed out the difficulties for law enforcement in identifying and locating malefactors in the anonymity of cyberspace.

The Internet, though, was a little different then. Fewer than 6 million American households had Internet access – dial-up, of course. Web-based retail sales amounted to a whopping $39 million annually – approximately what Sergei Brin and Larry Page made this morning. By way of comparison, the Census Bureau's latest estimate of e-commerce retail sales was more than $26 billion just last quarter.

Here we are 11 years later, and the future of the Internet shines brightly. Just an example – I got a chance the other day to watch a portly, hirsute young man in a bikini vamping it up in a satire of a Shakira video. Let me show you a clip. Think about it – more than 12 million people around the world have watched a video that a bunch of kids, not a major movie studio or television network, filmed in a single afternoon. User generated content like this is one of the many small miracles that the Internet serves up daily.

But one goal of these hearings is to anticipate the problems that new technologies can create for consumers. Take the clip, for instance. Is there a rating system to tell me whether it is appropriate for my young daughters? And how can we make sure that we continue to foster an environment where the next YouTube is able to flourish without confronting new tolls along the Internet superhighway?

From a law enforcement perspective, the global nature of the Internet poses one of our biggest challenges. The thorniest issues we face cross international boundaries: scammers calling Americans from abroad; spam and spyware, most of which is from foreign sources; and data breaches at overseas call centers.

---

[1] The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or of any other Commissioner.

Our challenge over the next decade is to figure out what useful role government can play in this global environment.

To be certain, for many consumer protection issues, private sector efforts are crucial. Companies that design secure software and firewalls. ISPs that filter spam. Organizations like Spamhaus, Stopbadware, the Anti-spyware Coalition, TrustE, and the Anti-Phishing Working Group. Their efforts aren't limited by national boundaries, and they've benefitted consumers around the globe.

But government is not irrelevant by a long stretch, especially because it defines when conduct is unacceptable. For instance, state laws requiring notification of security breaches have exposed vulnerabilities that existed for years under the radar screen. Just ask Choicepoint. When breaches never became public, there wasn't much incentive to get the problems fixed. And in the early days of the Internet, it wasn't certain that it was illegal to send unsolicited commercial email. The CANSPAM legislation – buttressed by the FTC's own enforcement – made the ground rules crystal clear. In the coming decade, though, we in government will have to be creative about reconciling the borderless Internet with our bounded authority – whether through information exchanges, beefed up alternative dispute mechanisms, or cooperation with private groups working to fix the same problems.

Make no mistake – no matter what else happens, the FTC's law enforcement role will be critical. The civil penalty authority Congress granted us in CANSPAM gave our antispam efforts real teeth. Sadly, in spyware cases, we don't yet have that authority. Why does this matter? Consider a company like 180 Solutions (now calling itself Zango) which placed more than 6.9 billion pop up ads on consumers' computers without notice or consent. Many came from major corporations who, I hope, would be shocked and dismayed if they knew how their Internet ads were reaching American consumers. Right now, all we can do is get disgorgement of profits, but we can't fine the malefactors at all. What kind of deterrence is that?

If Congress really wants to enhance consumer protection in the next decade, it needs to come up with a consensus anti-spyware law that gives us the authority to penalize the purveyors of spyware. And we at the Commission need to start "naming names"– that is, releasing the names of companies whose dollars, perhaps inadvertently, fuel the demand side of the spyware problem. Nothing would be more effective, I think, than having the CEO of a corporation open the morning newspaper, learn that his company's ads are reaching consumers' computers via spyware, pick up the phone and call his subordinate to say, "Don't let this happen again. Ever." In the Zango case, we're taking a useful first step – sending letters to the major advertisers who used Zango to deliver pop-ups, so they'll know – if they didn't already – how their ads were delivered, and how not to advertise in the future.

Spyware, spam, and their ilk are not the only issues we're concerned about, of course. If we in America are truly to achieve the promise of the Internet, people will need to have meaningful access to the vast breadth of Web-based applications and content. That's why the Net Neutrality debate is so important. So to those who ask why we're undertaking a study of Net Neutrality, I say, how could we not? Both consumer protection and competition issues are at play here – a combination at the core of what the FTC does.

Some of the most important issues regarding Net Neutrality involve transparency and disclosure. Will carriers block, slow, or interfere with applications or services? If so, will consumers be told all of this before they sign up? To my mind, failure to disclose these limitations would be "unfair or deceptive" in violation of the FTC Act.

Net Neutrality also invokes complicated competition issues. The last mile of the Internet is its least competitive. Nearly all homes in the US – upwards of 98 percent – that receive broadband get it either from their cable or telephone company. Up until now, the relative neutrality of the Internet has meant that competition and innovation elsewhere in cyberspace has not been affected by the market power of the telephone and cable companies. But if these companies are able to discriminate, treating some bits better than others, there is a danger that their market power in the last mile can interfere with the growth, character, and development of the Internet.

To be sure, there is another side to the debate. The ability of providers to charge more for time sensitive applications and content that takes up more broadband may encourage them to make necessary investments. That's a goal that all of us should support.

I'm lucky: I can raise these questions without providing answers – ones, by the way, that I don't necessarily have. Like you, I'll be looking for solutions to the problems of the future from our experts today. Hopefully, Woody Allen will be proven right: they'll involve cream pie and hot fudge.