IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE: VERIZON INTERNET SERVICES, INC. Subpoena Enforcement Matter RECORDING INDUSTRY ASSOCIATION OF AMERICA 1330 Connecticut Avenue, NW Suite 300 Washington, DC 20036 v. VERIZON INTERNET SERVICES, INC. 1880 Campus Commons Drive Reston, Virginia 20191	Miscellaneous Action No. 1:03MS00040 (JDB)

DECLARATION OF PARRY AFTAB

I, Parry Aftab, pursuant to 28 U.S.C. § 1746(2), hereby declare under penalty of perjury as follows:

1. I make this declaration based upon personal knowledge. I am an Internet privacy lawyer and Executive Director of the WiredSafety.org ("Wired Safety"), the world's largest and one of the most respected online safety groups. I am also the author of the book, The Parent's Guide to Protecting Your Children in Cyberspace (McGraw-Hill, 2000) and A Parents Guide to the Internet (1997). I specialize in policy issues impacting the Internet, worldwide.

2. Wired Safety is a 501c-3 non-profit corporation and is the umbrella for WiredPatrol.org, WiredKids.org, and Cyberlawenforcement.org, all manned by unpaid volunteers. Wired Safety dedicates most of its time and efforts to teaching the public how to get the most out of the Internet and avoid being victimized online.[1] Our volunteers work towards that mission each and every day.

3. Our volunteers are specially screened and trained and provide one-on-one assistance when people are victimized online. Our cyber-911 help channels[2] are staffed 24/7 to provide immediate help in online emergencies. Cybercrimes are referred to law enforcement agencies which often ask for our assistance in their investigations. We find and report child pornography, assist in reporting sexual predators and cyberstalkers and protect people from predators, identity theft, cyberstalking, fraud, hacking attacks and privacy violation online. Our WiredKids program also educates parents, children and schools about online safety and privacy.[3]

4. We protect children, adults and senior citizens alike and teach them how to avoid, and defend themselves against, identity theft, fraud, security and privacy violations and online predators. Alarmingly, many of the steps that Internet users can take to protect themselves will be frustrated if someone can simply obtain their identity through the filing of a subpoena under Section 512(h) of the Copyright Act.

---

[1] Over 100,000 victims have received our help.
[2] Accessed through our Wiredpatrol.org front page or via IRC on the Wiredpatrol.org server
[3] For more information about our programs, visit http://www.wiredpatrol.org, http://www.wiredkids.org and http://www.aftab.com

5. Armed only with an IP address and malice, a stalker, sexual predator, pedophile or perpetrator of online fraud and identity theft will easily be able to pierce the veil of anonymity otherwise afforded to Internet users. This would permit any individual – including those acting in bad faith or worse – to submit a subpoena to the clerk of a court without the supervision of a judge or the due process protections afforded by the courts. That is why we have submitted this declaration in support of Verizon's position.

6. I have set forth various scenarios below that better describe the kinds of risks associated with allowing someone to easily obtain offline contact information.

7. Children and Online Sexual Predators. A sexual predator sits in a chatroom, waiting for the right child to enter. The child does. They always do. Thirteen years old, the young girl chats happily about her school, her softball team and her music. The sexual predator reaches out, "I love ___ [insert her favorite pop star] too!." The young girl bites, and the conversation begins. The sexual predator may be masquerading as a cute fourteen-year-old boy, or another young teen girl. But no matter what persona he takes on, it is with the single goal of meeting this girl offline, for sexual exploitation. And, with between 12% and 24% of the teen girls[4] surveyed admitting to meeting online acquaintances offline, in person, the risk of his being able to succeed is very real.

[4] The largest survey conducted in connection with teen girls and their Internet activities was conducted jointly by our online safety group (under our former name) and Drs. Berson (husband and wife team from University of South Florida) and surveys 10,800 teen girls between the ages of 12 and 18. Most of the participants were between the ages of 13 and 16. More information about the survey can be found at http://www.ntia.doc.gov/ntiahome/ntiageneral/cipacomments/pre/aftab/surveysummary.htm. These surveys have been replicated offline in schools and the percentages range from 12 – 14% admitting to meeting Internet acquaintances in real life. Family PC Magazine, in the Spring of 2001 conducted their own smaller survey of teen boys and teen girls. They concluded that 14% of teen boys were meeting online strangers in

8. Those percentages would increase significantly if the predator knew how to contact the child offline and was able to easily obtain information about who the child is and where the child lives.

9. While the methods used by typical Internet-related sexual molestation differ from those used traditionally by offline sexual molesters and rapists, with universal access those lines are expected to blur. A few years ago, a violent child rapist used the Internet to find a map and layout of a boys' school dormitory. He used the plans to break in and rape young students in their dorms. How long before violent sexual molesters and rapists learn how to abuse the DMCA to obtain even more targeted information about a particular child? I fear, given the current learning curve, not long at all.

10. Little bits of information that children give away online, the name of their soccer team, or their school, or their girl scout troop number, or favorite baseball team can, when paired with other information, lead a sexual predator to the child's door.[5] That's why we are so adamant about children and teens not sharing personally identifiable information online with anyone they don't know in real life. Most children understand this and the risks involved. But if DMCA subpoena power is upheld, it won't make any difference how careful our children are.

11. Every day we hear about the latest case of a child lured into an offline meetings and raped. Or we learn that a young girl is killed. Every year the number of cases

---

real life and 24% of teen girls were doing so. With approximately 30 million minors online in the United States, this has serious ramifications.

where online sexual predators attempt to, and are successful in, luring a child into an offline sexual encounter increases exponentially. We rely on awareness of the importance of keeping personal information to yourself as our most powerful message in this war against Internet-related child molestation. If the broad application of the §512 subpoena is upheld, that message is now meaningless.

12. The ability of a sexual predator to easily obtain that child's address, family phone number and contact information would change everything. How do we protect children from the newest powertool in the sexual predator's arsenal? How long will it take for child molesters to realize how easy it is to obtain this information? (I regret having to raise this issue, since this affidavit itself will only help them understand how to abuse the system using the DMCA.) With one broad sweep, the DMCA subpoena power will frustrate the work of the entire online safety community to arm our children and their parents with cyber-street-smarts. It won't matter what they voluntarily or mistakenly give away. All the information the predators need can be obtained far more easily with the assistance of the local Federal District Court Clerk.

13. Common sense tells us that the sexual predators would never risk disclosing their real identities by making the application for the subpoena, especially in a courthouse. But common sense doesn't apply when Internet sexual predators are involved. Surprisingly enough, most Internet sexual predators use their real names when luring children into offline meetings. Some have been brazen enough as to brag about themselves and their notoriety, pointing the children (or

[5] A revised version of the online story known as "Shannon" that demonstrates the risks of children sharing personal information online can be found at http://www.wiredkids.org/safety/tiffany.html.)

FBI agents posing as a child) to articles in which they are featured. Identifying themselves to a clerk in the District Court wouldn't faze any of them. At least not if the end result is having the child's last name, address and telephone number delivered conveniently to their mailbox. It's worth the risk.

14. I will share a recent case, to show how far these men will go. Several months ago, a mother contacted our group. Her thirteen-year-old daughter was being blackmailed and had been forced to produce child pornography for someone she had met online. Her daughter was a "good girl" who follows the rules and never gets into trouble. She was aware of the risk of sharing her personal contact information, and never would have agreed to meet someone offline. Yet, the sexual predator managed to get to her anyway. (We will call this young girl "Susan" to protect her real identity.)

15. Susan received a message from someone online purporting to be another young girl in trouble. When Susan offered her help, the "young girl" said that she had been sexually victimized and didn't know where to turn. Susan, being a caring person, offered to help. She advised the "young girl" to talk with her mother about the problem. And when the "young girl" said it was hard to communicate about such intimate matters in writing, and asked for Susan's telephone number, Susan offered it to her. All the knowledge about how important it is not to give out your telephone number online didn't matter when a "young girl" needed help.

16. The "young girl" called Susan. But sounded more like a 50-year-old man. And he had no reservations about identifying himself as one. He told Susan that he "knew where she lived" and that unless she used her webcam to do unspeakable

things on camera where he could watch (and presumably record) her acts, he would come to her home and rape and kill her. If she told her mother, he threatened to rape and kill them both. He would call and threaten her repeatedly if she didn't answer his cell phone calls on the first or second ring. She was terrorized for months -- and complied with his demands for months. Finally she broke down and confided in her mother. When her mother reached out to this man, he threatened to kill her as well. We turned this case over to the FBI's Innocent Images unit and the Internet Crimes Against Children task force in her region. But this is the kind of thing that happens more often than anyone would ever believe. Sexual predators will do anything they can to reach a child offline. We shouldn't be making it easier for them to do so.

17. Cyberstalking and Harassment "I know where you live and I am going to kill you.", "I know what route your children take home from school…", "Interested in "doing" nine-year-old twins?", and "I am watching you…and like your new blue pajamas". Messages like these and others arrive through our cyber-911 cyberstalking help form, and in our live help channels daily.[6] Technology, such as Trojan horses, allows someone to send you an infected file that allows them to watch you through your webcam or listen to you in your own home using your computer's sound card, without your knowledge.[7]

[6] Readers Digest in April, 2000 published a special article on cyberstalking, highlighting our work under our former name. (The name of our cyberstalking help group is now WiredPatrol.org.) Their press release about the article can be found at http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=105&STORY=/www/story/03-28-2000/0001176125.

[7] CourtTV in its 2002 Safety Challenge special dealt with Trojan horses and risks of cyberstalking using Trojan horses to record people in their own homes, secretly. You can view videoclips from that special from the link provided at http://www.aftab.com.

18. Cyberstalkers are typically seeking revenge or retribution for some real or imagined wrong. Those who are the most persistent (and among the most dangerous) often have romantic or sexual fixations on the victim of the cyberstalking or harassment. It is essential that the ability of the cyberstalker to locate or contact the person offline is as limited as possible. Cyberstalking victims know this, and work hard to keep their offline identities and contact information private. Their hard work would be thwarted quickly if all their stalker needed to do was walk into a courthouse and fill out a form, swearing falsely that they held a valid copyright that was being infringed.

19. Parties to marital and family court disputes, battered and abused women and widows and widowers are often the targets of cyberstalking and harassment. They live with death threats, hacking attacks, websites that solicit sex on their behalf, and defamatory postings, sometimes daily. Allowing their predators to reach through the IP address to confirm their identity and the new online identities they have been forced to hide behind would be irresponsible.

20. Law Enforcement and Online Investigations Our Cyberlawenforcement.org division is run by volunteers who are or used to be members of law enforcement. I serve on the Home Office cybercrime task force on their law enforcement and cybercrime prevention committees. We also work very closely with law enforcement, and frequently assist in their online investigations.

21. Law enforcement counts on anonymity online. Larger national and international agencies often have special IPs and online accounts that can't be traced back to

them. But smaller and regional law enforcement agencies often do not have this kind of identity protection when the IP-address is pierced.

22. Law enforcement agents often sit in child pornography chatrooms and channels in connection with child pornography and child sexual exploitation investigations and sting operations. They go undercover as a child to ferret out child molesters online. These investigations take months or even longer. How long would it be before child molesters and child pornographers would learn to use the DMCA subpoena power to "check out" a new visitor or "child victim" in their channels and chatrooms? What about when law enforcement is investigating cyber-terrorism? Death threats or bomb threats? Even criminal copyright activities? It is ironic that a tool being sought by copyright holders could be used to frustrate the prosecution of criminal cases enforcing their rights.

23. From my many years of work on the important issues of online safety and security, I believe that the safety and privacy of all Internet users, and ability of the law enforcement community to protect us online, would be in placed in grave jeopardy.

24. There are less intrusive ways to provide the protection sought by copyright owners than by putting the privacy and safety of Internet users at risk. Surely we shouldn't have to choose between the two important rights of property protection and safety. We strongly support the protection of intellectual property rights online and offline, but if the subpoena under Section 512(h) of the Copyright Act is permitted to apply as proposed, the public's privacy and safety would be sacrificed. That is too high a price to pay in my opinion.

25. Pursuant to 28 U.S.C. § 1746(2), I, Parry Aftab, hereby declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge, information, and belief.

Parry Aftab, Esq.
Executive Director, WiredSafety
and Wired Kids, Inc., in individual
capacity and on behalf of
WiredSafety

EXECUTED ON MARCH 17, 2003