

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

v.

Case No. 06-CR-65

PETER T. OLSON,

Defendant.

REPLY TO DEFENDANT’S MOTION TO SUPPRESS

The Defendant, Peter T. Olson, by his attorney, Robin Shellow, of The Shellow Group hereby replies to the Government’s Response to Defendant’s Motion to Suppress. The Government in its Response asserts that even short-term subscriptions to websites whose names are allxboys.com and erectboys.com were suggestive of child-pornographic content. The Government also asserts that subscriptions to the websites mentioned above are enough for probable cause. With respect to both arguments, the Government has intentionally, like an ostrich, *kept its head in the sand*.

A. What’s In a Name?

1. *Girls, Girls, Girls*

The Government asserts in its Response, that the use of the word “boy,” in a website could connote gender, but probably denotes age. A short trip to the 42nd Street subway stop in mid-town Manhattan, where the streets are ablaze with signs that read GIRLS GIRLS GIRLS, XXX GIRLS, need not be undertaken. A Google search for the names of strip clubs within 150 miles of Milwaukee reveals that popular gentleman’s clubs featuring exotic dancers bear such names as Naughty Girls (Oshkosh), Lollipops

(Portage, WI), Girls Girls Girls (Madison), Little Darlings (Kalamazoo, MI), Wisconsin Dolls (Wisconsin Dells, WI), Showgirls I, and Showgirls III (Hammond, IN).¹ Are we to infer from these names that these establishments feature minors? It would be an impermissibly weak inference to conclude that, based on these names, customers enter these establishments searching for, or hoping to find, criminal child exploitation.

From Hammond to Oshkosh, no strip club could be found called Women Women, Women nor Naughty Women, nor Show-Woman I, nor Show-Woman III. “Girl” is the industry’s term for female, just as “boy” is the industry’s name for male. The Government’s recourse to the dictionary’s common usage definition of the word “boy” makes no sense in the specialized context of the sex industry’s use of the term. See Response at p. 6, note 3.

2. *Boy Oh Boy*

A search of a popular online dating service called Millionaire Match, voted best of the Web by Forbes Magazine and the Wall Street Journal, in a banner advertising their on-line services, beckons ICE agents and others with the tantalizing slogan, “Meet Cute Boys.” Another dating site BB (Big and Beautiful) has an advertising slogan called “Meet Big Boys.” A simple search for the term “boys” in Google results in, *boys in the hood, the beastie boys, the beach boys, back-street boys, bus-boys, office boy, messenger boy, whipping boy* and of course, *Boy George*.

B. The Time Interval between Olson’s Subscription and the Regpay Investigation is Not Overstated and Does Defeat Probable Cause

Olson does not overstate the extent of the time interval between the time ICE agents reviewed the websites and the time Olson subscribed to them, any more than the

¹ <http://www.stripclublist.com>

Government understates such time interval. Olson bought his first membership in a suspect website in July 2002 and his last one in November 2002. ICE agents investigated the websites in July-August 2003. Based on these dates, the lapse of time between Olson's membership purchase and the ICE investigation of websites may have been between 8-9 months and 12-13 months, depending on which websites Olson subscribed to first and which websites ICE investigated in July and which in August.

Olson insists that the proper moment in time from which to measure the time interval is the date of his purchase of membership, not the date of the lapse of such membership, as the Government proposes. The date of membership purchase is the only date cited by the agent in the Affidavit. Assuming that Olson used the websites once he subscribed to them, the date of membership purchase constitutes the date of the last, indeed the only, known use of each website by Olson. Any later use of a website by Olson is speculative only.

The time lapse must be measured from Olson's last known use, which is the date of membership purchase. *See United States v. Wagers*, 2006 U.S. App. LEXIS 16070; 2006 FED App. 0209P (6th Cir.) (appellate review of *United States v. Wagers*, 339 F. Supp. 2d 934 (E. D. Ky. 2004)). In *Wagner*, the Court of Appeals stated that the inference that the websites contained child pornography was "more tenuous" when the agents investigated and found child pornography just 5 months after the suspect's last known use. *Wagers*, 2006 U.S. App. LEXIS 16070 at 8. Pursuant to *Wagner*, a similar inference in the instant case would be so tenuous as to be invalid, whether the time lapse is 8 or 9 months.

Measuring the time lapse from the date the membership expired would require the judge issuing the warrant to stack inferences by (1) inferring that Olson still actively used the websites around/at the time his membership expired, and (2) that the time lapse between the time ICE investigated the websites and Olson may have used them (providing the first inference was correct) was short enough to legitimately infer that the websites contained illegal matter at the time of such inferred use. Such inference-stacking would make the inferential link far too tenuous to justify a finding of probable cause.

C. Subscriptions to Websites that Contained the Word Boy and the Letter X are Insufficient to Establish Probable Cause

1. The Government Knew That the Information Contained In the Olson Application Could Result In the Search and Arrest of Persons for the Unknowing Possession of Child Pornography

There can be no question that every adult, from an experienced ICE agent to an experienced Bloomingdales.com on line shopper, knows that “x” means “sex.” The websites subscribed to by Olson contained the universally known “x” as a means of communicating the sexual content of the websites. Beginning in 2000, Yahoo and other major internet service providers endorsed the creation of the XXX web in an effort to segregate, by domain name, those sites that have sexual content.² But sexual content is not illegal. Child-pornography is illegal.

The Government in its Response suggests that the Court not minimize the credentials and experience of Special Agent Kurkowski, who was a child pornography expert. It is the Government’s responsibility to pass on to its agents information material

² Code-abiding Porn to Get.xxx Domain, <http://www.washingtonpost.com/wp-dyn/content/article/2005/06/02/AR2005060201927.ht>

to their investigative techniques and to not ignore the evolving problems of the knowing-vs.-unknowing possession of child pornography.

The Government relied in its application solely upon the names of the websites and on subscriptions to websites that contained pornographic images of adults and that possibly may have contained some images of children (although it is entirely unknown if or how many) somewhere within them (although it is anyone's guess where and how visible) at the time of such membership.

The application was made in bad faith. The affiant failed to include any fact in the application suggesting that Olson intended to possess child pornography. Yet the Department of Justice had known since October 13, 2003, about a common practice in the adult web industry called mouse-trapping, that results in the unintentional possession of child pornography by those who visit adult pornographic websites. This information was not included in the Affidavit.

John G. Malcolm, Deputy Assistant Attorney General, Criminal Division of the United States Department of Justice, testified before the Senate Judiciary Committee on October 15, 2003, one year before the Olson Application, regarding the unknowing possession of child pornography. Yet, the applications for warrants did not reflect that change in the technology that makes unintended possession of child pornography through mixed websites much more likely than it had been in the early days of the internet.

Malcolm testified:

Over the last several years, online pornographers have used various technological and marketing techniques designed to trick both adults and children into viewing their offensive material. One favorite trick of online pornographers is to send pornographic spam email. Another is to utilize misleading domain names or deceptive metatags (which is a piece of text hidden in the Hypertext Markup Language (HTML) used to define a web page) which can mislead search engines

into returning a pornographic web page in response to an innocuous query. As a result of these deceptive metatags, searches using terms such as Atoys,@ Awater sports,@ AOlsen Twins,@ ABritney Spears,@ Abeanie babies,@ Abambi,@ and Adoggy@ can lead to pornographic websites. Indeed, it has been estimated that ninety percent of children between the ages of 8 and 16 have been exposed to obscene material on the Internet. **Moreover, once an unsuspecting person is on a pornographic website, online pornographers utilize other techniques such as Amousetrapping@ to prevent that individual from exiting these websites and stopping the assault of offensive material.**³ (emphasis added)

Pornography accounts for a fifty-seven billion dollar global industry. Porn revenue is larger than all combined revenues of all professional football, baseball and basketball franchises. Twelve percent of all websites on the internet contain pornography. Twenty-five percent of total search engine requests every day are pornographic in nature.⁴

After Assistant Attorney General Malcolm's testimony on mouse-trapping, it is infinitely clear that subscription to any random adult web-site may result in the unintended and unwitting possession of child pornography. Thus, an affidavit in support of a search warrant cannot be sustained unless there is additional evidence that the subscriber knew from the content of the home page of the web-site he specifically subscribed to, that it probably contained sexual depictions of children. Mouse-trapping is a marketing tool specifically developed by adult website purveyors that makes any subscriber a potential victim of the unknowing possession of child pornography:

A related service is providing consumer Internet traffic to another adult Web site in return for a small per-customer fee. Such "traffic forwarding" is similar to the fees paid through CPC traffic referrals, except that the consumer is forwarded involuntarily (i.e., without an affirmative choice to be forwarded). This practice is known as "mousetrapping" (or "selling exit traffic" in the industry),

³ Indecent Exposure: Oversight of DOJ'S Efforts to Protect Pornography's Victims, Presented on October 13, 2003, Testimony of John G. Malcolm

⁴ Pornography Statistics, www.familysafemedia.com/pornography_statistics.html.

and a mousetrapped user who tries to leave a sexually explicit site is automatically forwarded to another such site. This other site may be operated by a different operator, but that fact is irrelevant to the user who just wants to get out. (Technically, mousetrapping refers to a process enabled by JavaScript (a scripting language for Internet browsers) in which the closing of one window automatically directs the user to another Web page. The second Web page can do the same, so that attempting to exit the second page spawns a third page, and so on.

The Government in its Response shares some details of the investigation of Regpay, but fails to point out that the seizure of the credit card subscription information led to the Government amassing a huge data base of 70,622 domestic subscribers and 25,597 foreign subscribers to websites that contained pornography. Attorney General Ashcroft himself described that “Regpay allegedly processed over three million in credit card payments for hundreds of websites, **many** of which provided child pornography.”⁵

The Government knew at the time it applied for the Olson Warrant that many of the Regpay sites linked users to other sites that contained child pornography and thus, in this case, the failure to advise the magistrate of that information constitutes bad faith. The Regpay investigation yielded information that child pornography was advertised on 11 of the 50 sites operated by Regpay.⁶ While the site operator can choose what to advertise on what particular page of a website, a viewer’s only way of protection is to avoid pornographic web-sites entirely.

A site whose home page included uncensored sexually explicit images and links allowing the user to see other pages on the site without payment is clearly not taking precautions against minors viewing sexually explicit material—and there are many such sites available on the

⁵ Leaders of Global Internet Child Pornography Operation Plead Guilty, <http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2005&m=March&x=200503011650...>

⁶ See above Cite, at page 3.

internet. But there is a range of precautions that can be taken, and no objective standard for “what is enough.” Some of these precautions include offering a text-only page describing the contents of the site in general terms and a warning that one must not be a minor to proceed further. However, nothing prevents a site taking such precautions from also providing free entry to sexually explicit imagery.⁷

Twelve months before the Olson Application, a wire service dedicated to articles about information technology, transmitted to every on-line computer magazine, including Wired, PC World, and Computer Age, all of which are regularly relied upon as reliable sources of news on information technology, that internet sites in Russia were using stealth technology to transmit pornography to unwitting home workstations. One month after the leaders of Regpay were indicted and splashed across the banners of hundreds of information Technology websites, the following article appeared:

Trojan Peddles Porn While You Work: Spammers Turn PCs into Porn Hosts without Owners' Knowledge

Internet sites, based in Russia are using stealth and a sophisticated new trojan program to turn home workstations into unwitting hosts in a pornography and spam distribution ring, according to security experts. The deceptive and potentially illegal practice came to the attention of experts in late June and has been a topic of conversation among spam fighters on Internet discussion groups since then, according to Joe Stewart, senior intrusion analyst with LURHQ, a Chicago-based managed security services company. Experts observed that one spammer who was sending out spam e-mail pointing to spoofed Pay Pal Web sites and Russian pornography sites appeared to be able to change the addresses of his Web sites every few minutes, according to Richard Smith, an Internet security and privacy consultant based in Boston. Smith stumbled upon the problem in early July while investigating e-mail messages pointing to a phony Pay

⁷ Youth Pornography and the Internet, Dick Thornburgh and Herbert S. Lin

Pal site that was being used to harvest personal financial information from customers of the online payment service.⁸

The Government had knowledge of both mouse-trapping technology and Trojans long before the Olson Application and knew that persons who subscribed to (a) adult web-sites and (b) Russian Web-sites were probably likely to have unwittingly possessed child pornography. Finally, the Government knew that an image, even one never sought-after or intentionally possessed by the user, remains for recovery by the Government indefinitely, despite efforts by the user to the contrary. Thus, the failure to share with the issuing magistrate the Government's knowledge that Olson could have unwittingly, and thus innocently, possessed child pornography constitutes bad faith. Such failure resulted in the warrant application containing only the information found in the Olson Application, exposing Olson to a search despite the fact that the Government knew that he might have been exposed to child pornography without ever indenting such exposure, and despite the lack of any evidence that Olson had ever been exposed to child pornography or had sought such exposure.

2. The Affidavit Failed to Support Probable Cause

The Affidavit did not provide the crucial and relevant information outlined above, which constituted the totality of the circumstances the magistrate should have considered in deciding whether probable cause existed.

The Affidavit alleged no facts indicating that Olson was a consumer of child pornography or that Olson fit the profile or possessed characteristics of child pornography offenders, as the government concedes on page 8 of its Response.

⁸ New Trojan Peddles Porn While You Work, http://computerworld.hu/hirek_hir.php?id=32117, July 13, 2003.

The Government correctly states that probable cause does not require proof beyond a reasonable doubt. Response at p. 8. However, the Government incorrectly asserts that the meager information alleged in the Affidavit, based on all the circumstances, established a “fair probability” that evidence of criminal child exploitation would be found on Olson’s computer. Id.

The information of Olson’s paid memberships in pornographic websites that months later contained child pornography somewhere (possibly in out-of-the-way locations), the information of typical traits of child pornography offenders, and the information of Olson’s frequent use of his home computer may have created a certain possibility that Olson was a child pornography offender, but did not create a “fair probability” that he was one. See R. at. 8.

It takes a very strained inference indeed to assert that anyone who had subscribed to pornographic websites that 6 months later contained child pornography was “fairly probable” to have been a child pornography offender, merely because that person frequently used their computer and because child pornography offenders share certain traits not found in the person in question. Such a strained inference simply does not support a “fair probability” that the person was an offender and that the evidence of such offense would likely be found of their computer.

In Olson’s case the meager facts restated by the Government on page 8 of its Response constitute the totality of the circumstances, or all of the circumstances, offered for the magistrate’s consideration. These circumstances differ greatly from those found in *Wagers* (where the suspects had had a prior conviction for similar criminal conduct) and do not support probable cause.

It is respectfully requested that this Court grant Olson's previously filed Motion to Suppress.

Dated at Milwaukee, Wisconsin August 15, 2006

Respectfully submitted,
Peter Olson, Defendant

_____/s/ Robin Shellow_____
Robin Shellow #1006052

P.O. ADDRESS

324 W. Vine Street
Milwaukee, WI 53212
(414) 263-4488