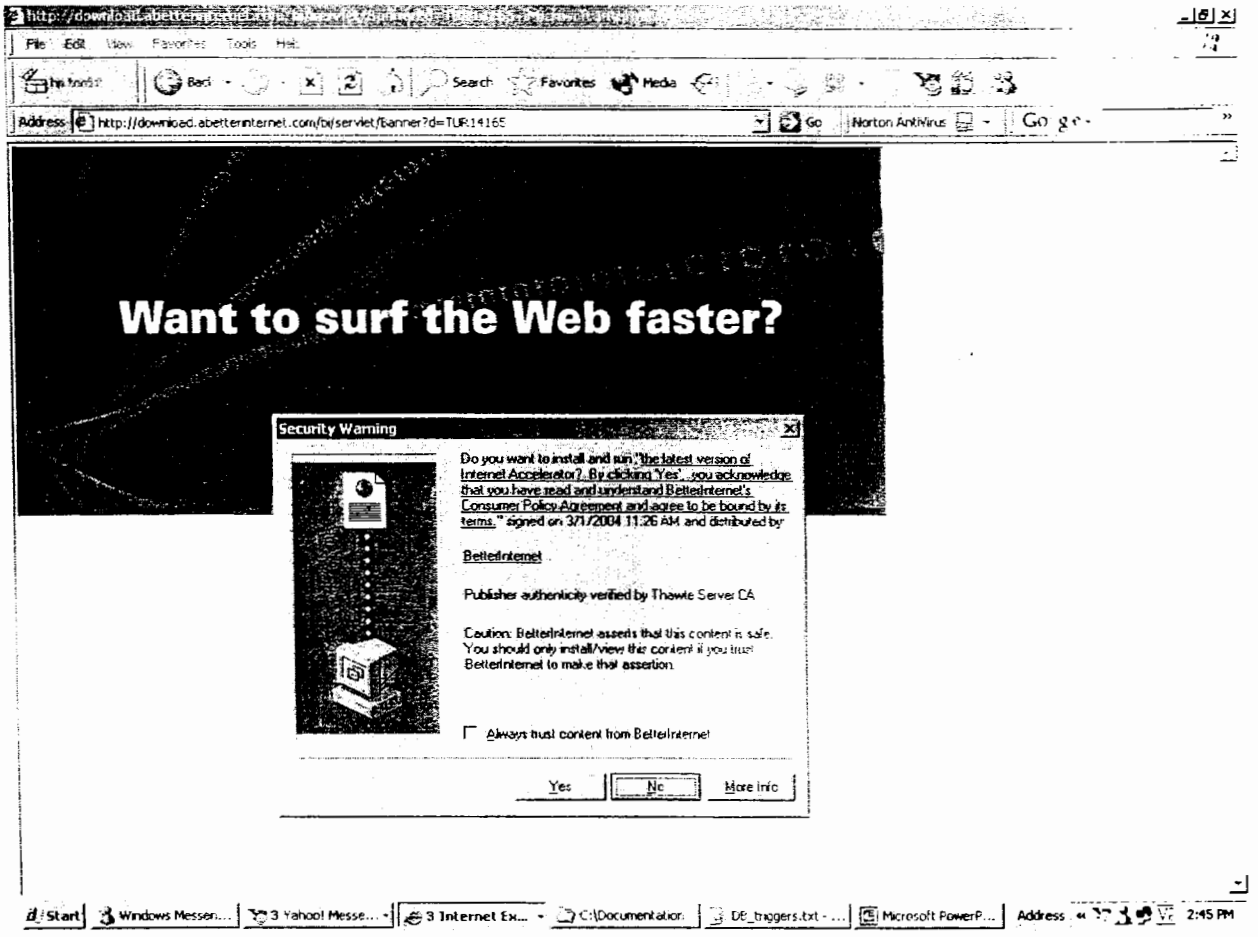
EXHIBIT 73

From: Chris Dowhan
Sent: Monday, April 12, 2004 11:30 AM
To: alan@direct-revenue.com; joshua@direct-revenue.com; rod@direct-revenue.com; dan@dkcp.net
Subject: legal questions
Attach: OffenseDefenseOverview.ppt

Hi Guys.
Josh and I had put together a few thoughts that I had meant to get out to everyone before this morning, but it may still be useful as follow with the lawyers. One item we did not touch on in that meeting is whether our MachineID data is considered personally identifiable or in any way a breach of our position on privacy.

- C

We place ads on various networks

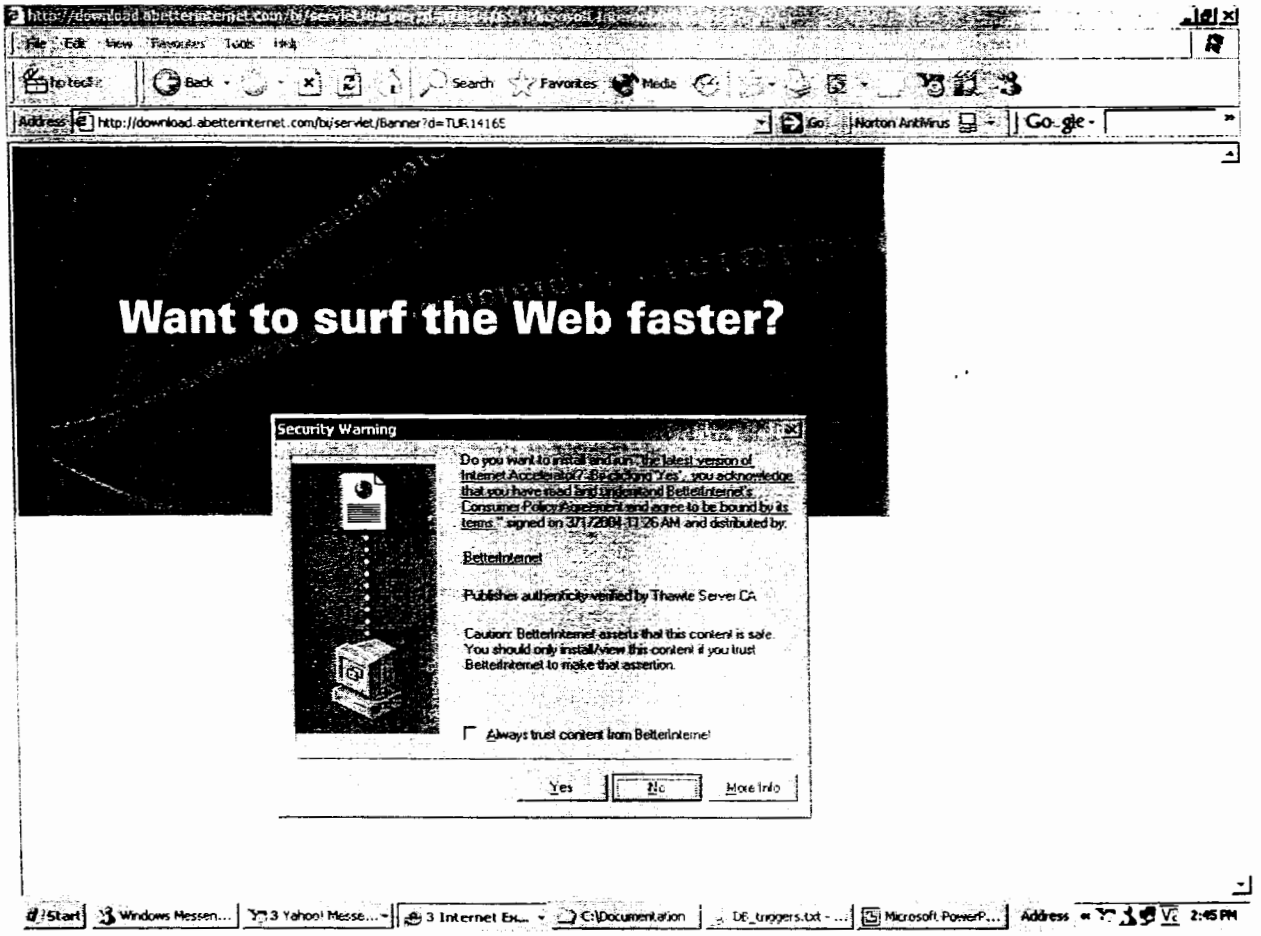


The goal is to get to the download as quickly and efficiently as possible. The ad impressions come in all shapes and sizes, some without images, some activating a download only after a mouseover or a click on an image. The Security Modal box that references our Ts and Cs is seen by all downloaders *except* those with low security settings – we estimate approximately 1% of surfers.

1) Is this a legal loophole for end-users who want to claim they didn't opt-in? We can't currently differentiate those that saw the modal versus those that had low enough security settings to allow *any* download to get through.

2) Do low security settings == acceptance? It clearly says in the screen where you control the settings "Most content is downloaded and run without prompts."

We have bundle partners



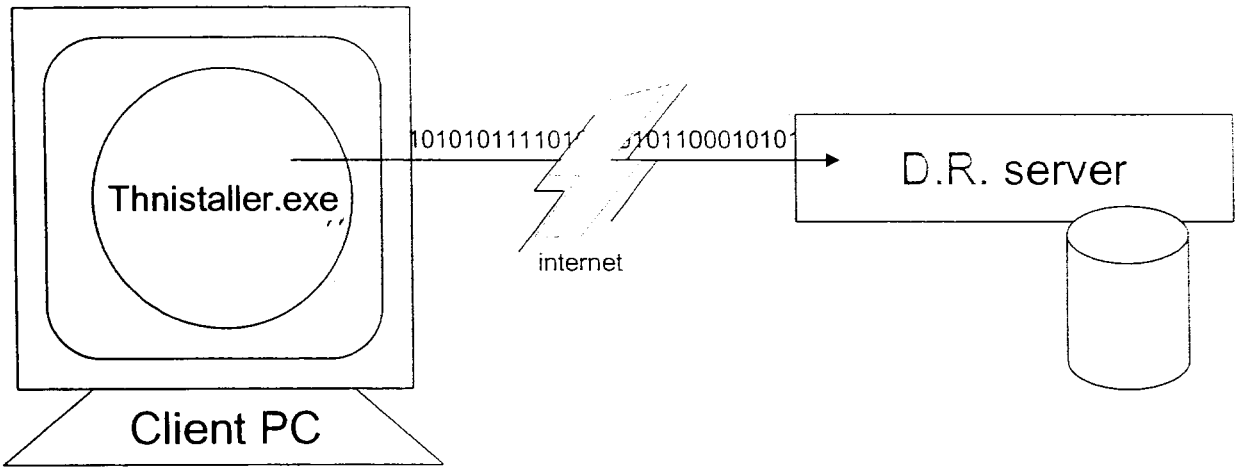
Our bundle partners have a clear and strict directive that the end-user must be presented with our Ts and Cs and opt-in before our app can be downloaded to the machine. Our only record that they have complied is the fact that a download and install occurred – we have no explicit knowledge of an opt-in because we don't require acceptance of terms during the install itself, only during the download. Also, we do not monitor their live distribution efforts to see that they are in compliance.

1) In the event of non-compliance, even if we can point the finger at the distribution partner for breach of our contract, does that still put the validity of our user agreement at risk?

2) If we can segregate our user base by users from each distributor, would any exposure be limited to only those users acquired through this channel? or any bundle deal download?

3) Would the same be true for a bad distribution partner who exploits known Microsoft security holes?

The Thinstaller: Data Collection

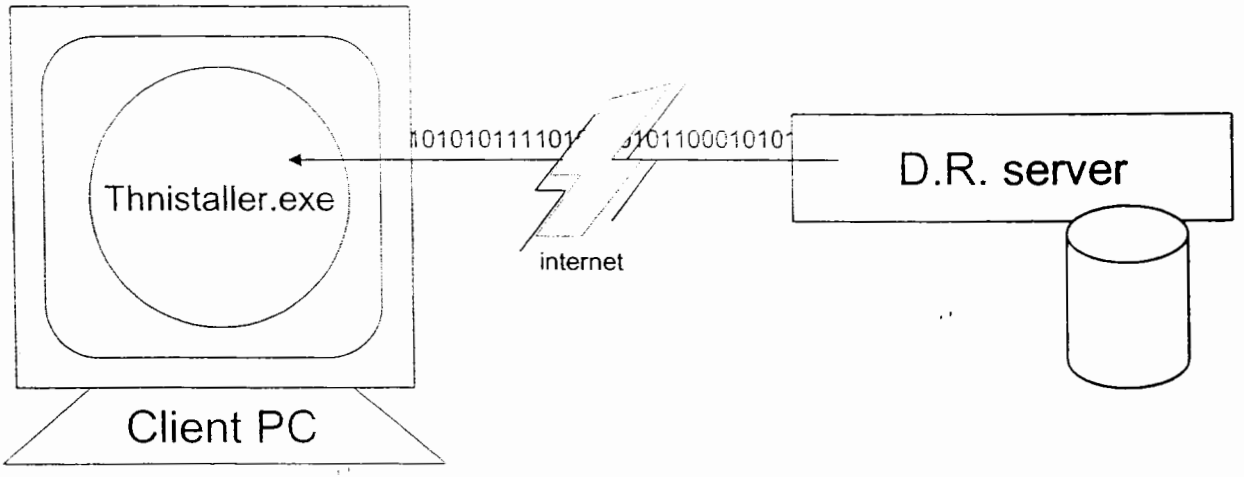


The Thinstaller is our application that enables "smart" installing behavior. It gathers information about the client PC and sends it into our servers where we make a decision on what, if anything, we should download. The information is, for the most part, OS, Browser Type, what apps are installed, and what apps are running. In addition we grab the following as our way of tracking unique installs. It is not personally identifiable.

- SerialID - The Volume serial number can be checked by running "vol" from the command prompt
- MAC Address - On Win 2000 and XP MAC address can be checked by running "ipconfig /all" from the command prompt. On Win 9x the program is called winipcfg.
- ProductID - The Product ID is displayed in My Computer properties.

1) Is there anything here that would cross the line between acceptable and a target for privacy advocates?

The Thinstaller: Protecting our Install



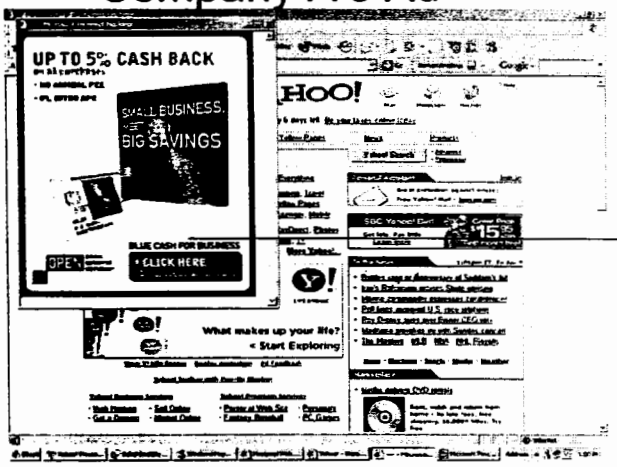
Currently we respond to a thinstaller by downloading the Utility that was advertised when the client PC initiated the download, plus our ad client if we don't see that one is already on the machine. Going forward we would like to use the information gathered (OS, Browser Type, what apps are installed, and what apps are running) to also do the following:

- Identify known competitive software and disable or remove it prior to download – basically pave the way for a successful install
- Do ongoing monitoring of these types of apps to keep the ad client installed until the user visits our uninstall website (demo of myPCtuneup.com)
- Pave the way for partner apps such as the 404 handler, etc. and install them on compatible desktops

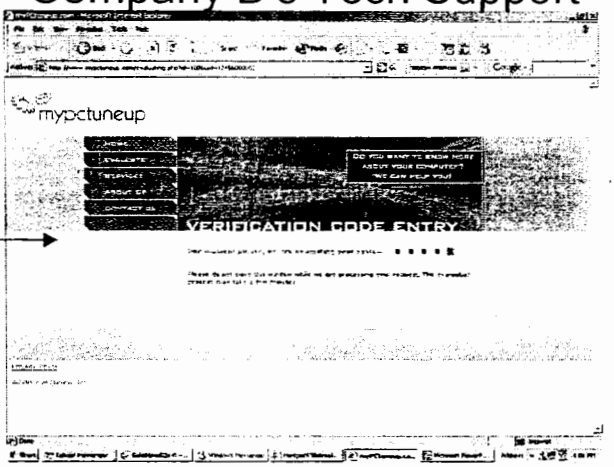
1) When it comes to protecting our installation against removal, Is there any differentiation between a competitor's app, a competitor's app that is aggressive (tries to remove us – if we could prove it!), adware-removing software like Adaware (assuming we could get around it as opposed to disabling it)?

The Cross-Sell

Company A's Ad



Company B's Tech Support



We will be branding all ads and provide a way for users to uninstall. I'm not sure if there will be a link directly to our uninstall site or an intermediate "splash" page where there is more information prior to the uninstall link – I suppose legislature may dictate the exact way the link must work.

Once at our uninstall site we intend to try and cross-sell users to a Tech Support service. We would like to use data to increase conversion – data collected prior to this visit and/or stored on the user's PC by us and/or data collected at that moment but sent to us through a mechanism installed prior to the visit (probably software installed by our ad client).

1. Does an "uninstall software app" that gets installed by Company A need to be branded as Company B if we intend to use it beyond the uninstall process of Company A's software? What constitutes an uninstall? During uninstall we would expect to leave the apps that are not specifically our ad client – e.g. 404 error handlers, search bars.
2. What would we need to say in our EULA to allow Company A to share info with Company B through a software app like this, or from data collected and stored in a database on the server?
3. Assuming that the data is not more personally identifiable than what was described earlier in this doc, would there be any other restrictions on data that is sharable?

Thoughts

- Should we explore having Ts and Cs baked into the thinstaller so that during install they are revealed? This is terrible for us because it is disruptive to bundle deals where the consumer opts into a combined value proposition of Utility+Ads, and to bake in Ts and Cs would mean knowing up-front exactly what the value is that they are agreeing to in exchange for seeing Ads.
- Leaving a remnant on the machine is the only way to know on future install attempts whether or not this is the same machine that has already uninstalled our ad client. It creates continuity needed to know whether or not changes have taken place on the machine that would alter it's identity for us. Is that a valid argument for leaving behind software? That said, we would expect to reinstall the ad client for all users in that situation who did not sign up for the Tech Support service during uninstall, so would that negate the argument?

Utopia

User agrees to multiple Ts & Cs combined during one opt-in

Pave path for all installs, disabling competitors (whether there is technical conflict or not)

After the opt-in we pull down our apps (any and all that were in the EULA) whenever we want – whenever it is convenient. Not necessarily right after the opt-in during the first download

Fortify machine and protect all of our installed apps against attack, including any app that tries to remove us outside of our uninstall website process

When a user uninstalls by following a link to our uninstall website, we would uninstall only that app associated with the link they followed.

There might be a residual piece or pieces of code that stay behind for future ID purposes. Also, there might be a shared app among all of our downloaded products that stays. This app might stay and try to prevent competitive apps from monetizing this machine because they would still pose a threat to our apps that are still there, or an app that we intend to roll out.