iPhone Applications & Privacy Issues: An Analysis of Application Transmission of iPhone Unique Device Identifiers (UDIDs)

Eric Smith[*]
http://pskl.us

October 1, 2010

Abstract

Every Apple iPhone shipped since its introduction in 2007 contains a unique, software-visible serial number -- the Unique Device Identifier, or UDID. Apple provided this functionaly to allow application developers to uniquely identify the iPhone being used for purposes such as storing application preferences or video game high scores. While the UDID does facilitate the process of collecting and storing certain types of data, it also creates a tempting opportunity for use as a tracking agent or to correlate with other personally-identifiable information in unintended ways. In this paper, we investigate where and how UDIDs are being shared, with whom, and how the UDIDs are being used.

Tags: iPhone, Apple, Privacy, UDID, Application Development, Information Security, Tracking, GPS Data

[*] **E**ric Smith is the Assistant Director of Information Security and Networking at Bucknell University in Lewisburg, Pennsylvania. He has over 15 years of field experience in information security, networking, and systems administration. He has provided consultation services in places such as Research Triangle Park and New York City. Eric is a founding member of PreSet Kill Limit, the security research group which has won the Defcon Wardriving Contest several years in a row. Eric can be reached at eric@pskl.us.

Table of Contents

Figures

Tables

Executive Summary

In 1999, Intel released its newest CPU -- the Pentium 3. Each processor included a unique serial number, visible to any software installed on the system. A product backlash quickly developed as privacy rights groups realized that this serial number could be used to track users' online behavior. The industry, along with trade groups and governments, blasted this new feature; many governments went as far as proposing legislation to ban the use of Pentium 3 CPUs. Following the outcry, Intel quickly removed the serial number feature from their processor line, never to be re-introduced.

Fast forward a decade to the introduction of Apple's iPhone platform. Much like the Pentium 3, devices running the Apple iPhone operating system (IOS), including Apple iPhones, iPads, and iPod Touches, feature a software-readable serial number – a "Unique Device Identifier," or UDID. In order to determine if the privacy fears surrounding the Pentium 3 have manifested themselves on the iPhone platform, we studied a number of iPhone apps from the "Most Popular" and "Top Free" categories in Apple's App Store. For these applications, we collected and analyzed the data being transmitted between installed applications and remote servers using several open source tools. We found that 68% of these applications were transmitting UDIDs to servers under the application vendor's control each time the application is launched. Furthermore, 18% of the applications tested encrypted their communications such that it was not clear what type of data was being shared. A scant 14% of the tested applications appear to be clean. We also confirmed that some applications are able to link the UDID to a real-world identity.

The iPhone's UDID is eerily similar to the Pentium 3's Processor Serial Number (PSN). While the Pentium 3 PSN elicited a storm of outrage from privacy rights groups over the inherent risks associated with the sharing of such information with third parties, no such concerns have been raised up to this point regarding the iPhone UDID. As UDIDs can be readily linked to personally-identifiable information, the "Big Brother" concerns from the Pentium 3 era should be a concern for today's iPhone users as well.

Introduction & Background: Privacy Concerns and Unique Serial Numbers

Pentium 3 Processor Serial Numbers

In 1999, Intel released its newest CPU -- the Pentium 3. In addition to numerous performance enhancements, Intel also added a new feature: a unique serial number, burned into each and every CPU. Intel hoped that their Processor Serial Number (PSN) would not only be a boost to online commerce, but also attract business and government interest as it would allow for better asset tracking and resource allocation. According to Intel, the "PSN will be used in applications that benefit from stronger forms of system and user identification, such as (a) Applications using security capabilities, (b) Manageability, and (c) Information Management."[1]

The PSN did in fact attract a lot of attention -- but not the sort Intel had envisioned. It was blasted by both industry and government as an unnecessary intrusion on the privacy and security of people using PSN-enabled computers as it facilitated tracking of users without their knowledge or permission. These concerns lead the European Parliament to recommend to their member states legal measures against the sale of this CPU in order to "prevent these chips from being installed in the computers of European Citizens."[2] Computer manufacturers reacted almost immediately by adding a software switch in the BIOS to allow the PSN feature to be disabled. Shortly thereafter, Intel removed the PSN feature from the Pentium 3 line, and they have not reintroduced it into any of their subsequent products. The microprocessor industry quickly abandoned the notion of including a software-visible serial number into any of their devices.

Apple iPhones & Unique Device IDs

On January 9, 2007, Apple entered the cellular telephone market with the introduction of the iPhone. Possessing many of the abilities of an internet-connected laptop computer, the iPhone quickly became one of the most popular and influential devices in the cellular phone market. With over 59 million iPhones sold to date[3], iPhones are everywhere. Apple subsequently expanded their product line to include the iPod Touch and the iPad, both of which run the same software and share many of the same hardware features as the iPhone. For the purposes of this paper, "iPhone" refers to any device in the iPhone/iPod Touch/iPad device family.

Much like the Pentium 3 CPU, each Apple iPhone is equipped with a unique, application-visible serial number called a Unique Device ID (UDID). According to Apple, the use of UDIDs allows businesses to "ensure that devices continue to comply with required policies."[4] Application developers are encouraged to remotely query and store the UDID of any devices which run their applications. As an example, Apple suggests that the UDID is ideal "when storing high scores for a game in a central server." Apple's software development kit reference guide mentions that any software developer "...may use the UDID, in conjunction with an application-specific user ID, for identifying application-specific data on your server."[5]

The intended role of the UDID as a unique token to remotely store local application preferences is a convenient tool for programmers, but the potential for the abuse of privacy is remarkably high. Apple addresses this concern in their application development guide:

[1] http://www.intel.com/support/processors/pentiumiii/sb/CS-007579.htm

[2] http://www.cnn.com/TECH/computing/9911/29/eu.p3.ban.idg/index.html

[3] http://en.wikipedia.org/wiki/File:IPhone_sales_per_quarter_simple.svg

[4] http://www.apple.com/iphone/business/docs/iPhone_Business.pdf

[5] http://developer.apple.com/library/ios/#documentation/UIKit/Reference/UIDevice_Class/Reference/UIDevice.html

> "For user security and privacy, you must not publicly associate a device's unique identifier with a user account."[6]

While Apple promotes the use of the "uniqueIdentifier" API as a development tool, there is nothing in place which prevents these same application developers from using UDIDs as a tracking agent -- nor are there any restrictions in place to prevent companies from sharing this data with one other. Have the fears of nonconsensual user tracking stemming from Pentium 3 unique hardware serial numbers materialized on the Apple iPhone platform?

Recent Privacy Issues & User Concerns

Over the past few months, there has been renewed concern about online privacy by both individuals and the media after several popular sites have experienced large data breaches. High-profile leaks in social media sites such as Facebook[7] and Twitter[8] have illustrated to many day-to-day Internet users just how much of their personal information is in the hands of entities that may not be doing a good job of keeping that data private and secure. For many technology firms, it is substantially more profitable to collect and share personal information than it is to work to keep private data private. Furthermore, most users have given their consent -- albeit uninformed -- when they agree to the often-cryptic and constantly-changing terms of service imposed by the majority of sites which require an account to use their services. Twitter's privacy policy, for example, states that they have the right to share a user's private information, "such as your IP address, browser type, the referring domain, pages visited, and search terms" with any "trusted third parties" as they see fit.[9]

The usage data that many companies collect such as their users' IP addresses, browser types, referring domains, pages visited, search terms, length of visits, and so on is extremely valuable to advertisers and corporate marketing departments. While users might not be concerned that Twitter, for example, stores this information, they may be less comfortable knowing that they have given Twitter permission to share this information with anyone whom Twitter considers to be a "trusted third party."

Recently, the major web browsers have introduced privacy-enhancing features into their products. Mozilla's Firefox introduced the "Start Private Browsing" option, which prevents browsing history entries, persistent cookies, and cached objects from being saved after the web browser is closed. Google Chrome's "Incognito" mode, Microsoft Internet Explorer's "InPrivate Browsing", and Safari's "Private Browsing" features offer similar privacy protections as well.[10]

While these features help to mitigate some privacy concerns, they are not a panacea and they do not work on all platforms. Even with web browser advancements, online privacy advocates find themselves in a continual cat and mouse game with those who wish to profit from the demise of online privacy. The resulting avalanche of new tracking technologies is somewhat alarming. The Electronic Frontier Foundation's "Panopticlick" experiment proved that the browsing habits of users can be reliably tracked even in environments where private browsing settings were enabled. System attributes such as screen resolution, clock offsets, and time zone are being combined with classical metrics including cookies and IP addresses to construct an online profile which can be reliably tied to the browsing habits of an individual user, even with the most stringent privacy settings enforced.[11]

The privacy arms race on the iPhone platform, however, is remarkably one-sided. Safari's mobile version, the only web browser available, does not include any privacy features: no "Private Browsing" functionality, no ability to block or clear application cookies, and no access to the local browser cache. In addition to application-specific browser cookies, applications downloaded from Apple's App Store have access to the phone's Unique Device ID (UDID). An advertiser or other entity who wants to track user behaviors and patterns online could not ask for a better identifier than one that is guaranteed by the hardware manufacturer to be unique to a single device. There is

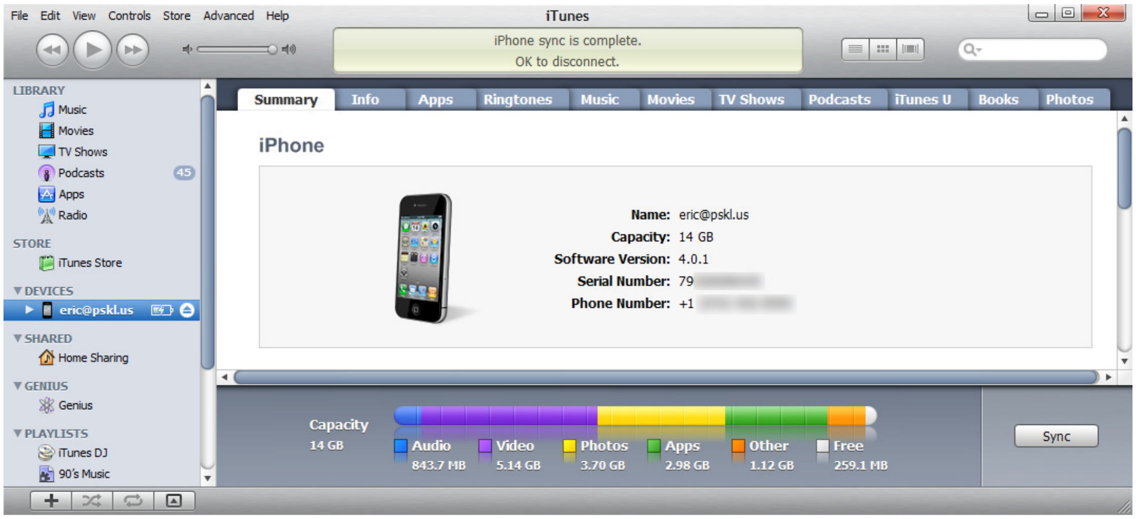
[6] http://developer.apple.com/library/ios/#documentation/UIKit/Reference/UIDevice_Class/Reference/UIDevice.html
[7] http://www.technewsworld.com/story/70515.html?wlc=1285255579
[8] http://mashable.com/2010/09/22/twitter-meltdown-17-year-old/
[9] http://twitter.com/privacy
[10] http://support.mozilla.com/en-us/kb/private+browsing
[11] https://panopticlick.eff.org/ and 9/21/2010 How Unique Is Your Browser?, Proceedings of the Privacy Enhancing Technologies Symposium (PETS 2010), Springer Lecture Notes in Computer Science.

no ability to block the visibility of the iPhone's UDID to any installed applications, nor is there a mechanism to prevent the transmission of the UDID to third parties in the current version of Apple's IOS, the operating system used by the iPhone.

Methodology

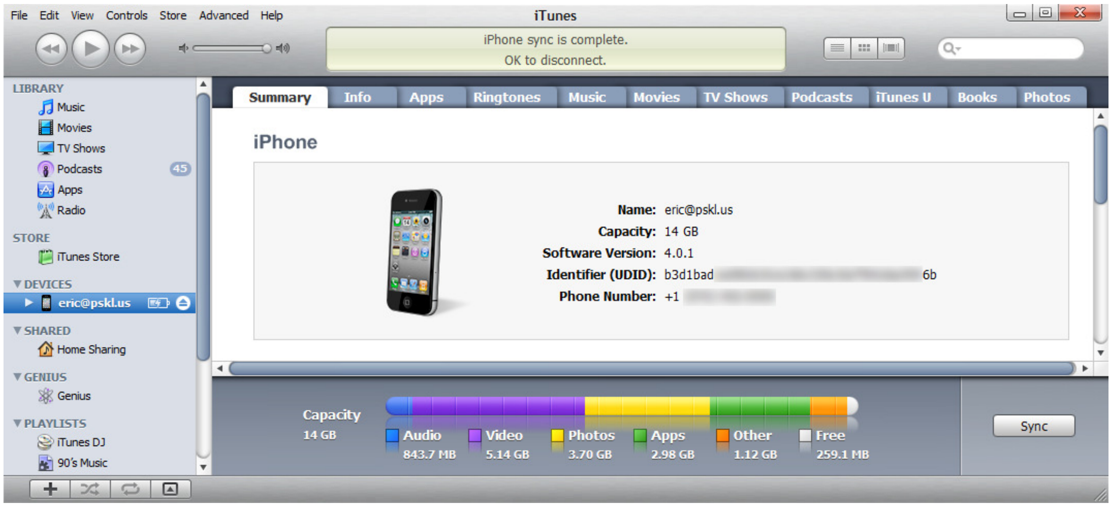
To determine whether UDIDs were being shared with vendors, we installed several applications on an Apple iPhone with a valid AT&T cellular subscription. As a starting point, the applications featured under the "Top 25 Free" category of Apple's App Store were downloaded and installed to the test device. Additionally, several news applications featured under the "News: Top Free" heading and a number of other shopping, business, and financial applications were installed. A total of 57 applications were evaluated.

In order to first learn the UDID of the target iPhone, it was connected via USB to a Microsoft Windows 7-based computer. The latest version of Apple's iTunes was installed; the phone was then allowed to synchronize with the local iTunes database. The UDID was then revealed by clicking the phone icon under the "Devices" heading and then selecting the "Summary" tab. (See Figure 1.) The device's hardware serial number is displayed. Clicking the serial number with the mouse will toggle the display to reveal the UDID. (See Figure 2.)



Name: eric@pskl.us
Capacity: 14 GB
Software Version: 4.0.1
Serial Number: 79[redacted]
Phone Number: +1 [redacted]

Figure 1: Apple's iTunes application, showing the attached phone's serial number.



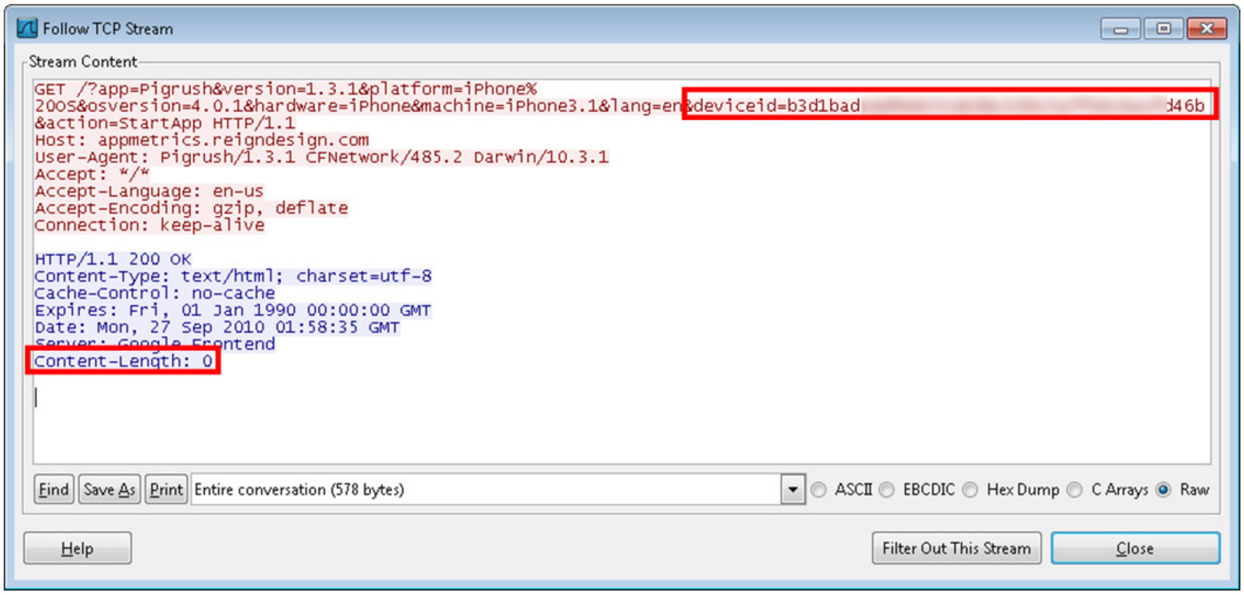
Name: eric@pskl.us
Capacity: 14 GB
Software Version: 4.0.1
Identifier (UDID): b3d1bad[redacted]6b
Phone Number: +1 [redacted]

Figure 2: Apple's iTunes application, showing the attached phone's UDID.

An internet connection was provided to the iPhone by means of a local wireless network which was configured so packet captures could be readily obtained. Packet captures were recorded using tshark[12], the console-based libpcap capture utility. The resulting files were then analyzed using a suite of open-source tools including Wireshark, ngrep, and the Perl Net::Pcap libraries[13] in order to determine what, if any, personally-identifiable information was being shared with third parties. We also investigated the use of browser cookies as a secondary tracking mechanism.

Results

Sixty eight percent of the applications evaluated in this study do in fact transmit the UDID back to a remote server, owned either by the application developer or an advertising partner. In several instances, the communications between the application and remote server were encrypted by the use of SSL. In these cases, we were unable to determine what type of data was being shared. Based on the trends observed in this study, it is likely that the UDIDs were transmitted to remote hosts in those applications which employ SSL. Complete results of UDID transmission tests across applications are presented in Appendix A and Appendix B.



```
GET /?app=Pigrush&version=1.3.1&platform=iPhone%
20OS&osversion=4.0.1&hardware=iPhone&machine=iPhone3.1&lang=en&deviceid=b3d1bad[redacted]d46b
&action=StartApp HTTP/1.1
Host: appmetrics.reigndesign.com
User-Agent: Pigrush/1.3.1 CFNetwork/485.2 Darwin/10.3.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Date: Mon, 27 Sep 2010 01:58:35 GMT
Server: Google Frontend
Content-Length: 0
```

Entire conversation (578 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 3: A typical UDID tracking conversation between an application and a remote server. Note the size of the response message at zero bytes, indicating that this communication was initiated by the application strictly for tracking purposes, and not to retrieve any sort of remote content.

A substantial number of applications collect both the phone's UDID and some form of user login data which ties to a stored user account. These applications, such as Amazon, Facebook or Twitter, inherently have the ability to tie a UDID to a real-world identity. This ability, combined with the demonstrated widespread collection of UDID usage data, illustrates the ease of real-time user tracking.

In order to determine the feasibility of linking UDIDs to real-world identities, a number of applications which have the potential to map UDID to user identity were studied to determine if they are actively collecting UDID data. The results of this study are presented in Table 1: UDID collection by applications requesting user credentials. Of the applications evaluated in this study that collected UDIDs, require users to log in, and have personally-identifiable information affiliated with user accounts, 30% clearly transmit UDIDs; the rest used SSL to encrypt data transmission.

[12] http://www.wireshark.org/docs/man-pages/tshark.html
[13] http://www.wireshark.org/, http://ngrep.sourceforge.net/, http://search.cpan.org/~kcarnut/Net-Pcap-0.05/Pcap.pm

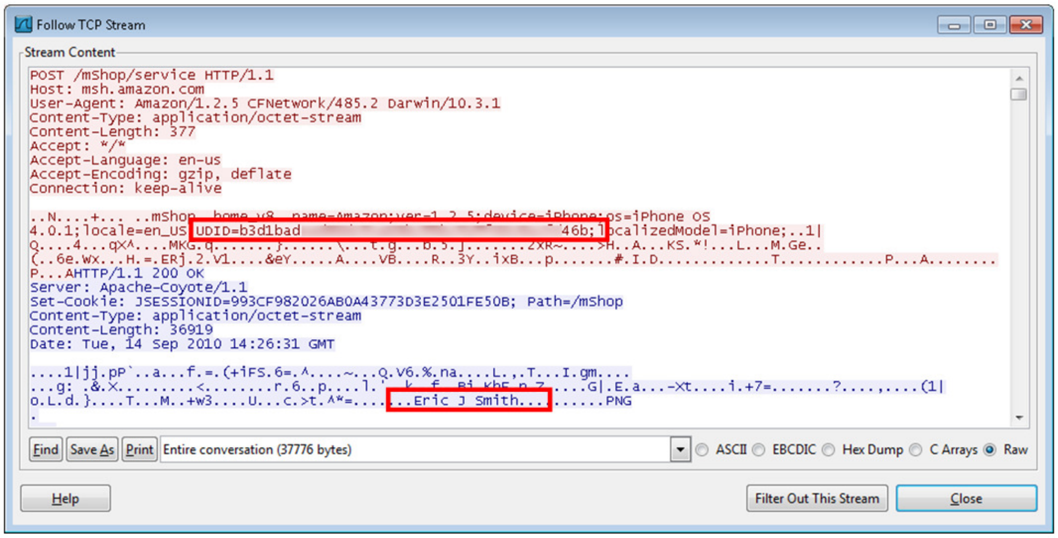
Table 1: UDID collection by applications requesting user credentials

Application	Transmits UDID?	Receiving Host
Amazon	Yes	msh.amazon.com
Chase Bank	Yes	cwf.chase.com
Target	Yes	target.122.2o7.net
Sams Club	Yes	samsclub.112.2o7.net
Best Buy	Unknown - SSL	
Barnes & Noble	Unknown - SSL	
Ebay	Unknown - SSL	
Paypal	Unknown - SSL	
Bank of America	Unknown - SSL	
Wells Fargo	Unknown - SSL	
Fidelity	Unknown - SSL	
American Express	Unknown - SSL	

Analysis

App Transmission of UDIDs

It is clear from this data that most iPhone application vendors are collecting and remotely storing UDID data, and that some of these vendors also have the ability to correlate the UDID to a real-world identity. For example, Amazon's application communicates the logged-in user's real name in plain text, along with the UDID, permitting both Amazon.com and network eavesdroppers to easily match a phone's UDID with the name of the phone's owner. The CBS News application transmits both the UDID and the iPhone device's user-assigned name, which frequently contains the owner's real name.

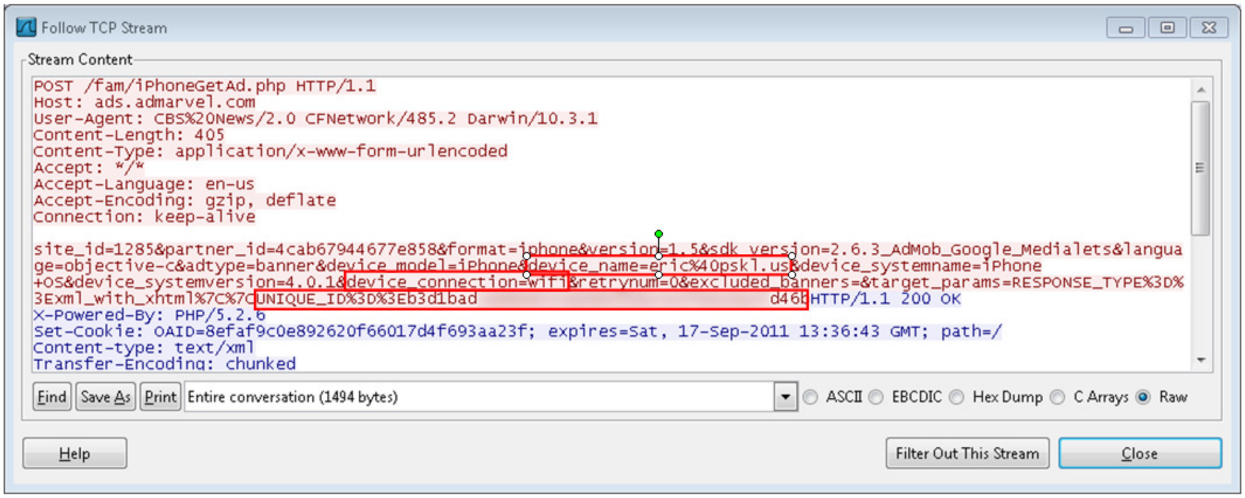


```
POST /mShop/service HTTP/1.1
Host: msh.amazon.com
User-Agent: Amazon/1.2.5 CFNetwork/485.2 Darwin/10.3.1
Content-Type: application/octet-stream
Content-Length: 377
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive

..N....+... ..mShop..home.v8..name=Amazon;ver=1.2.5;device=iPhone;os=iPhone OS
4.0.1;locale=en_US;UDID=b3d1bad[redacted]46b;localizedModel=iPhone;..1|
Q....4...qX^....MKG.q.......}......\...t.g...b.5.].......2XR~....>H..A...KS.*!...L...M.Ge..
(..6e.Wx...H.=.ERj.2.V1....&eY.....A....VB....R..3Y..ixB...p.......#.I.D............T...........P...A.......
P...AHTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=993CF982026AB0A43773D3E2501FE50B; Path=/mShop
Content-Type: application/octet-stream
Content-Length: 36919
Date: Tue, 14 Sep 2010 14:26:31 GMT

....1|jj.pP`..a...f.=.(+iFS.6=.^....~...Q.V6.%.na....L.,.T...I.gm....
...g: .&.X........<........r.6..p....l.'..k..f..Bj.KbE.n.Z.....G|.E.a...-Xt....i.+7=.......?....,....(1|
o.L.d.}....T...M..+w3....U...c.>t.^*=.......Eric J Smith..........PNG
.
```

Find   Save As   Print   Entire conversation (37776 bytes)   ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Help   Filter Out This Stream   Close

Figure 4: A conversation between the Amazon iPhone application and Amazon's servers. Note the transmission of the UDID to the remote host and the subsequent reply which contained the user's real name.

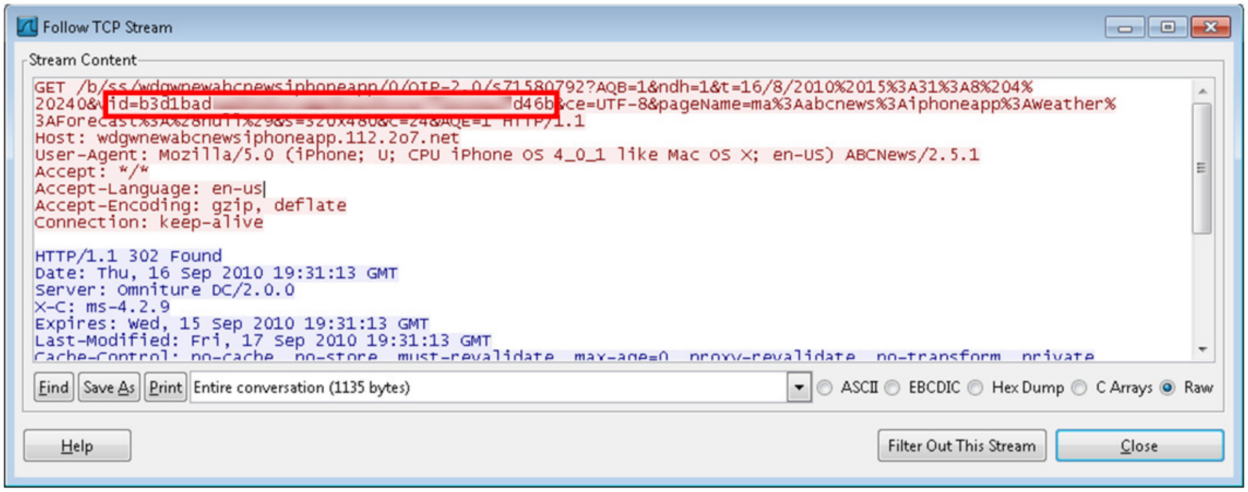


```
POST /fam/iPhoneGetAd.php HTTP/1.1
Host: ads.admarvel.com
User-Agent: CBS%20News/2.0 CFNetwork/485.2 Darwin/10.3.1
Content-Length: 405
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive

site_id=1285&partner_id=4cab67944677e858&format=iphone&version=1.5&sdk_version=2.6.3_AdMob_Google_Medialets&langua
ge=objective-c&adtype=banner&device_model=iPhone&device_name=eric%40pskl.us&device_systemname=iPhone
+OS&device_systemversion=4.0.1&device_connection=wifi&retrynum=0&excluded_banners=&target_params=RESPONSE_TYPE%3D%
3Exml_with_xhtml%7C%7CUNIQUE_ID%3D%3Eb3d1bad[redacted]d46bHTTP/1.1 200 OK
X-Powered-By: PHP/5.2.6
Set-Cookie: OAID=8efaf9c0e892620f66017d4f693aa23f; expires=Sat, 17-Sep-2011 13:36:43 GMT; path=/
Content-type: text/xml
Transfer-Encoding: chunked
```

Figure 5: Transmission of the UDID and device name by the CBS News app. Note that other data such as the connection type ("wifi") is also shared.

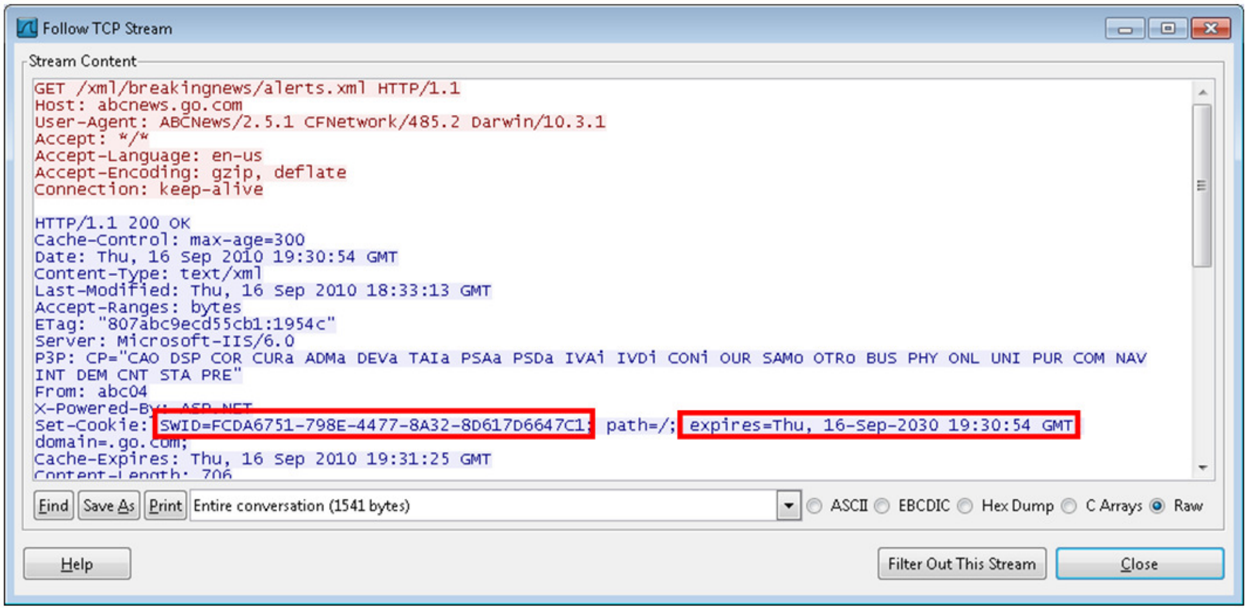
While some iPhone owners may purposefully want some trusted vendors to have access to their addresses, phone numbers, credit cards, and real names, they should be alarmed at the prospect of these same companies sharing their personal information with others. Is there any reason why the developer of a video game should know your home address?

Numerous applications were observed to transmit UDIDs while at the same time planting extremely long-lived tracking cookies onto the device. By setting cookies that don't expire for several years, companies are able to continue to tracking individuals' data for extended periods of time -- well beyond the lifetime of a single cellular device. For instance, the BBC News app includes a tracking cookie that expires in four years; ABC News' app cookie doesn't expire for twenty years. The existence of these long-lived persistent cookies could allow for third parties to link UDIDs from old, discarded phones to individuals' new phones as they upgrade to the newest iPhone model every few years.



```
GET /b/ss/wdgwnewabcnewsiphoneapp/0/OIP-2.0/s71580792?AQB=1&ndh=1&t=16/8/2010%2015%3A31%3A8%204%
20240&vid=b3d1bad[redacted]d46b&ce=UTF-8&pageName=ma%3Aabcnews%3Aiphoneapp%3Aweather%
3AForecast%3A%28null%29&s=320x480&c=24&AQE=1 HTTP/1.1
Host: wdgwnewabcnewsiphoneapp.112.2o7.net
User-Agent: Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_0_1 like Mac OS X; en-US) ABCNews/2.5.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 302 Found
Date: Thu, 16 Sep 2010 19:31:13 GMT
Server: Omniture DC/2.0.0
X-C: ms-4.2.9
Expires: Wed, 15 Sep 2010 19:31:13 GMT
Last-Modified: Fri, 17 Sep 2010 19:31:13 GMT
Cache-Control: no-cache, no-store, must-revalidate, max-age=0, proxy-revalidate, no-transform, private
```

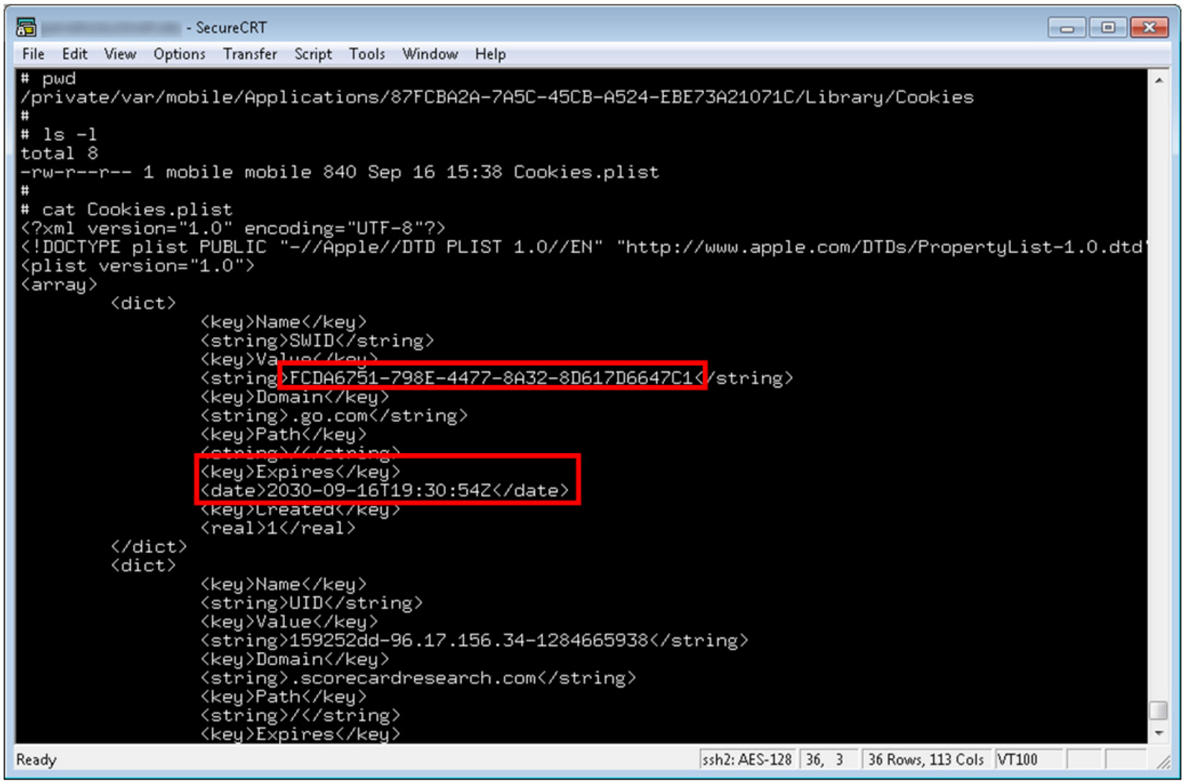
Figure 6: The ABC News app sends the UDID to a remote host.



```
GET /xml/breakingnews/alerts.xml HTTP/1.1
Host: abcnews.go.com
User-Agent: ABCNews/2.5.1 CFNetwork/485.2 Darwin/10.3.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 200 OK
Cache-Control: max-age=300
Date: Thu, 16 Sep 2010 19:30:54 GMT
Content-Type: text/xml
Last-Modified: Thu, 16 Sep 2010 18:33:13 GMT
Accept-Ranges: bytes
ETag: "807abc9ecd55cb1:1954c"
Server: Microsoft-IIS/6.0
P3P: CP="CAO DSP COR CURa ADMa DEVa TAIa PSAa PSDa IVAi IVDi CONi OUR SAMo OTRo BUS PHY ONL UNI PUR COM NAV
INT DEM CNT STA PRE"
From: abc04
X-Powered-By: ASP.NET
Set-Cookie: SWID=FCDA6751-798E-4477-8A32-8D617D6647C1; path=/; expires=Thu, 16-Sep-2030 19:30:54 GMT
domain=.go.com;
Cache-Expires: Thu, 16 Sep 2010 19:31:25 GMT
Content-Length: 706
```

Entire conversation (1541 bytes) ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 7: The ABC News webserver sets an app cookie with a 20-year lifetime.



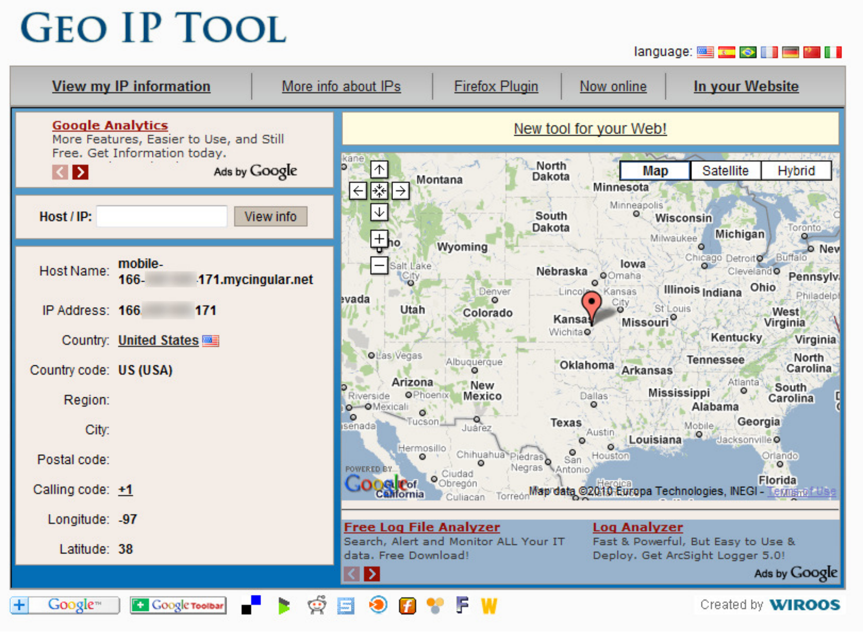
```
# pwd
/private/var/mobile/Applications/87FCBA2A-7A5C-45CB-A524-EBE73A21071C/Library/Cookies
#
# ls -l
total 8
-rw-r--r-- 1 mobile mobile 840 Sep 16 15:38 Cookies.plist
#
# cat Cookies.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd'
<plist version="1.0">
<array>
        <dict>
                <key>Name</key>
                <string>SWID</string>
                <key>Value</key>
                <string>FCDA6751-798E-4477-8A32-8D617D6647C1</string>
                <key>Domain</key>
                <string>.go.com</string>
                <key>Path</key>
                <string>/</string>
                <key>Expires</key>
                <date>2030-09-16T19:30:54Z</date>
                <key>Created</key>
                <real>1</real>
        </dict>
        <dict>
                <key>Name</key>
                <string>UID</string>
                <key>Value</key>
                <string>159252dd-96.17.156.34-1284665938</string>
                <key>Domain</key>
                <string>.scorecardresearch.com</string>
                <key>Path</key>
                <string>/</string>
                <key>Expires</key>
```

Ready | ssh2: AES-128 | 36, 3 | 36 Rows, 113 Cols | VT100

Figure 8: The ABC News app stores the tracking cookie in its application directory, not the Safari Cookies folder.

App Transmission of Location Data

While there is no direct evidence that this data is being used to physically track iPhone users, it would be trivial to implement such a system using a combination of UDIDs and time-stamped IP addresses. The correlation of this data with a GeoIP library[14] would allow an iPhone user's approximate physical location to be tracked in real time. The iPhone's hard-wired preference for local wireless networks over cellular data enhances this tracking ability, as the phone will only use the cell network for data when it has no wifi connectivity. While GeoIP lookups on cellular phone networks generally do not often provide useful location data, lookups on Wifi hot spots are often remarkably precise. See Figures 9 and 10.



Host / IP: View info

Host Name: mobile-166-[redacted]171.mycingular.net

IP Address: 166[redacted]171

Country: United States

Country code: US (USA)

Region:

City:

Postal code:

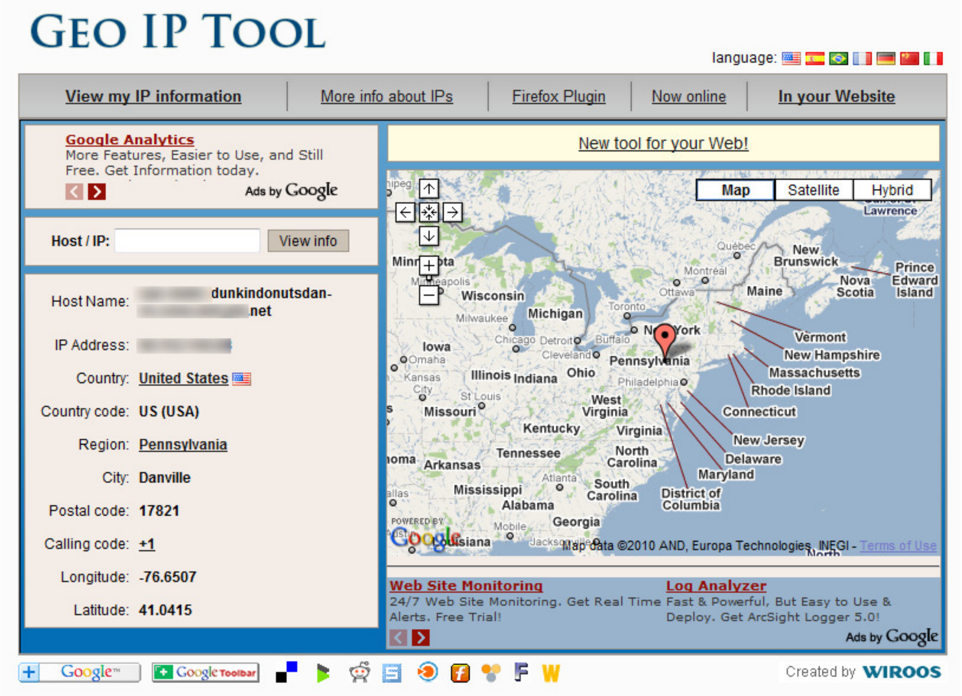
Calling code: +1

Longitude: -97

Latitude: 38

Figure 9: GeoIP lookup of a cellular-connected iPhones being used inside of a Dunkin Donuts restaurant in Danville, PA. Note that the location is reported incorrectly. Source: www.geoiptool.com.

[14] http://www.maxmind.com/



Google Analytics
More Features, Easier to Use, and Still Free. Get Information today.
Ads by Google

Host / IP:

Host Name: [redacted] dunkindonutsdan- [redacted] .net

IP Address: [redacted]

Country: United States

Country code: US (USA)

Region: Pennsylvania

City: Danville

Postal code: 17821

Calling code: +1

Longitude: -76.6507

Latitude: 41.0415

Web Site Monitoring
24/7 Web Site Monitoring. Get Real Time Alerts. Free Trial!

Log Analyzer
Fast & Powerful, But Easy to Use & Deploy. Get ArcSight Logger 5.0!
Ads by Google

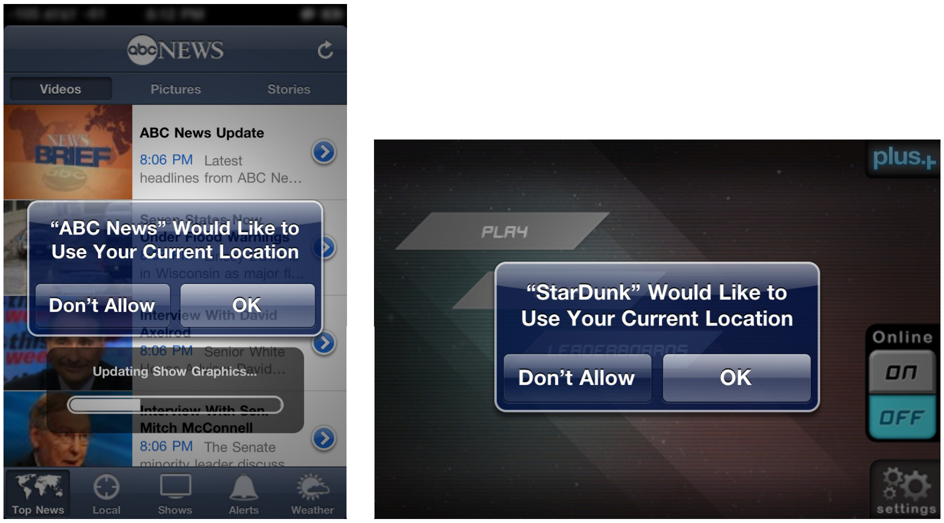
Figure 10: GeoIP lookup of the Wifi-connected iPhone being used inside of a Dunkin Donuts restaurant in Danville, PA. The reported location is correct. Source: www.geoiptool.com.

A number of the applications considered in this study requested access to the on-board GPS receiver. Several such applications – games, for example -- had no obvious need for this information. In several cases, applications which transmitted UDIDs were observed to transmit the iPhone's latitude and longitude as well. Even though the iPhone API requires that users give explicit permission to an application when it requests access to the phone's GPS receiver, users have already consented to this behavior. Apple's 159-page, single spaced terms of service states:

> *By using any location-based services on your iPhone, you agree and consent to Apple's and its partners' and licensees' transmission, collection, maintenance, processing, and use of your location data to provide such products and services.*[15].

Users cannot access content from Apple's App Store until they agree to these terms.

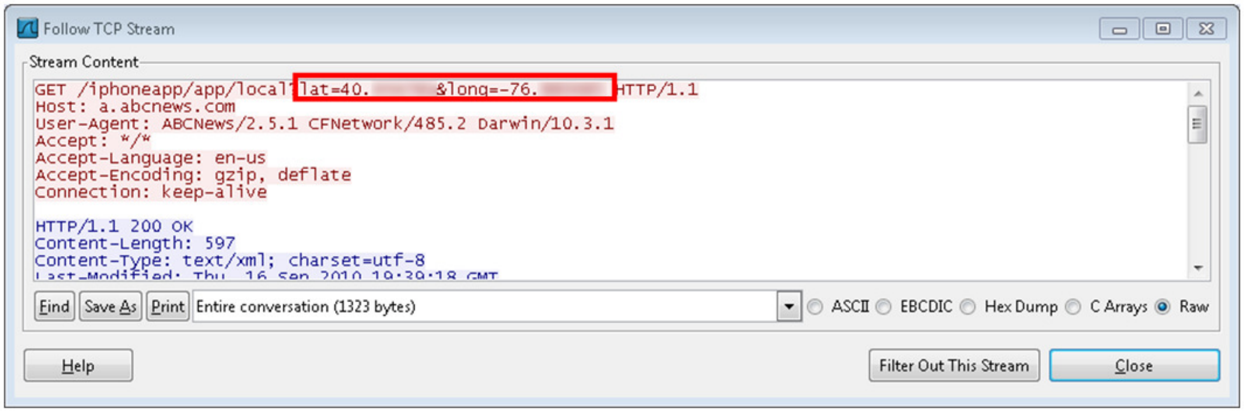
[15] http://images.apple.com/legal/sla/docs/iphone.pdf



“ABC News” Would Like to Use Your Current Location

“StarDunk” Would Like to Use Your Current Location

Figure 11: Examples of applications requesting the iPhone's GPS coordinates during startup



```
GET /iphoneapp/app/local?lat=40.[redacted]&long=-76.[redacted] HTTP/1.1
Host: a.abcnews.com
User-Agent: ABCNews/2.5.1 CFNetwork/485.2 Darwin/10.3.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 200 OK
Content-Length: 597
Content-Type: text/xml; charset=utf-8
Last-Modified: Thu, 16 Sep 2010 19:39:18 GMT
```

Entire conversation (1323 bytes) ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 12: The ABC News app transmits data back to remote servers. In this case, local content, such as weather is returned.

Conclusion

Privacy and security advocates, personal iPhone owners, and corporate iPhone administrators should be concerned that it would be feasible -- and technically, quite simple -- for their browsing patterns, app usage, and physical location collected and sold to unintended customers such as advertisers, spouses, divorce lawyers, debt collectors, or industrial spies. Since Apple has not provided a tool for end-users to delete application cookies or to block the visibility of the UDID to applications, iPhone owners are helpless to prevent their phones from leaking this information.

Since our study focused on applications which are available free of charge, it was not surprising to find that a large portion of the UDID leakage we observed was directly tied to advertisements and advertising networks. Several patterns emerged from our data which suggest that a handful of companies are in control of the in-app advertising market on the iPhone platform.

Table 2: UDID transmission by destination network

# of observed UDID Transmissions	Destination Network
11	Application vendor's network
9	data.flurry.com
5	adtest.qwapi.com - SSL Encrypted – Payload Unknown
4	admob.com
3	playhaven.com
3	tapjoyconnect.com / tapjoyads.com
2	2o7.net
2	admarvel.com
2	appspot.com
2	greystripe.com
2	medialytics.com
2	mobclix.com
1	fluentmobile.com
1	google-analytics.com

The iPhone's UDID is eerily similar to the Pentium 3's Processor Serial Number (PSN). But while the Pentium 3's PSN elicited a storm of outrage from the public and government over the inherent privacy risks associated with the ease at which a particular device can be remotely identified, no such concern has yet been raised about this same issue on the iPhone platform. Curiously, many of the same governments who threatened to ban the Pentium 3 in 1999 have since endorsed the use of the iPhone.[16] Since UDIDs can be readily linked to personally-identifiable information, the "Big Brother" concerns from the Pentium 3 days should be a concern for today's Apple mobile device users as well.

[16] http://www.reuters.com/article/idUSTRE6731VC20100804

Appendix A: UDID Usage by "Top Free" iPhone Applications, September 2010

App Name	Sends UDID?	Receiving Host	Host in HTTP Header	Reverse DNS	GeoIP Location	Netblock Owner
AIM Free	Yes	64.12.79.226	api.aim.net	apiaimnet-mtc-a.evip.aol.com		America Online
Amazon	Yes	72.21.210.121	msh.amazon.com	210-121.amazon.com	Seattle, WA	Amazon.com
APOD	Yes	216.74.41.4	data.flurry.com	441gift.com	Denver, CO	WCP/32POINTS INTERMEDIATE HOLDING COMPANY
BedIntruder	SSL	adtest.qwapi.com				
Bible	Yes	208.43.32.6	www.youversion.com	208.43.32.6-static.reverse.softlayer.com	Dallas, TX	SoftLayer Technologies
Bible	Yes	216.74.41.4	data.flurry.com	441gift.com	Denver, CO	WCP/32POINTS
Bungee Ball	Yes	216.74.41.4	data.flurry.com	441gift.com	Denver, CO	WCP/32POINTS
Coin Frenzy	Yes	204.236.231.106	ws.tapjoyconnect.com	Amazon EC2	Seattle, WA	Amazon.com
Color Fill	SSL	p19-buy.itunapple.com.akadns.net				
Dog Whistler	Yes	216.74.41.4	data.flurry.com	441gift.com	Denver, CO	WCP/32POINTS INTERMEDIATE HOLDING COMPANY
ESPN Score Center	Yes	198.105.194.203	m.espn.go.com	None	Burbank, CA	Disney Online
Fast Ball 2	Yes	174.129.209.2	iphone.playhaven.com	Amazon EC2	Lakewood, CA	Amazon.com
Flikster	Yes	209.237.23.55	api.flixster.com	pool4.flixster.com	San Francisco, CA	Unitedlayer
Flip Cup	Yes	216.74.41.4	data.flurry.com	441gift.com	Denver, CO	WCP/32POINTS INTERMEDIATE HOLDING COMPANY
Froggy Launcher	Yes	207.211.57.237	i.w.inmobi.com	87f-inmobi-vip1.	Andover, MA	ClearBlue Technologies
Galaxy on Fire	SSL	27-courier.push.apple.com				
Gravity Runner	Yes	174.129.209.2	iphone.playhaven.com	Amazon EC2	Lakewood, CA	Amazon.com
Heads will Roll	Yes	184.73.238.102	iphone.playhaven.com	Amazon EC2	Seattle, WA	Amazon.com
Hell Flyer	No					
I Bomber 2	SSL	ngpipes-balancer-115307477.us-east-1.elb.amazonaws.com				
iBasket Free	Yes	184.73.255.108	ws33.tapjoyconnect.com	Amazon EC2	Seattle, WA	Amazon.com

Fingerzilla	Yes	184.73.255.108	ws.tapjoyads.com	Amazon EC2	Seattle, WA	Amazon.com
Fingerzilla	Yes	72.167.232.192	inertsoap.com	p3nlh062.shr.prod.phx3.secureserver.net	Scottsdale, AZ	Godaddy.com
iLuvMozart	Yes	67.228.84.178	www.kooapps.com	piggybankgifts.84.228.67.in-addr.arpa	Seattle, WA	SoftLayer Technologies Private Residence
iLuvMozart	Yes	174.143.230.35	ads2.greystripe.com	None	San Antonio, TX	Iris Experience S. L.
iSniper	No					
Jewel Smash	Yes	202.213.218.116	web.comm.mininat.com	None	Japan	So-net Entertainment Corporation
Mirror Free	SSL	adtest.qwapi.com				
Mr. Giggle	SSL	24-courier.push.apple.com				
Mr. Runner	SSL	adtest.qwapi.com			Andover, MA	NAVISITE
Ninja 7	SSL	adtest.qwapi.com				
Pigrush	Yes	74.125.93.121	appmetrics.reigndesign.com	qw-in-f121.1e100.net	Mountain View, CA	Google
Pimple Popper	SSL	adtest.qwapi.com				
Red Laser	Yes	76.74.154.88	redlaser.com	api2.occipital.com	Los Angeles, CA	Peer 1 Network / ServerBeach
Scramble CE	Yes	74.114.8.115	74.114.8.115	None	San Francisco, CA	ZYNGA GAME NETWORK
Skyburger	No					
Groupon	Yes	184.73.223.62	asotrack1.fluentmobile.com	Amazon EC2	Ashburn, VA	Amazon.com
Groupon	Yes	74.125.93.101	www.google-analytics.com	qw-in-f101.1e100.net	Mountain View, CA	Google.com
Stair Dismount	No					
StarDunk	Yes	204.236.197.115	data.mobclix.com	Amazon EC2	Pipersville, PA	Amazon.com
Stunt Lite	No					
Super KO 2	No					
Talking Tom	Yes	173.194.35.141	outfit7-affirmations.appspot.com	lga15s16-in-f141.1e100.net	Mountain View, CA	Google
Tap Zoo	Yes	74.125.91.141	streetviewtapzoo.appspot.com	qy-in-f141.1e100.net	Mountain View, CA	Google
Text Plus 4	Yes	184.73.250.242	ws.tapjoyconnect.com	Amazon EC2	Seattle, WA	Amazon.com
Trapster	Yes	173.203.24.249	www.trapster.com	None	Cardiff By The Sea, CA	Rackspace Hosting / Trapster.com

TV Quizzle	Yes	174.143.230.35	ads2.greystripe.com	None	San Antonio, TX	Iris Experience S. L.
Void	SSL	p19-buy.itunes.apple.com				
We City	Yes	184.73.110.103	data.mobclix.com	Amazon EC2	Seattle, WA	Amazon.com
Zombie Duck Hunt	Yes	165.193.245.52	a.admob.com	Amazon EC2	Seattle, WA	Amazon.com

Appendix B: UDID and Cookie Use by iPhone News Apps

App Name	Type of Data Sent	Remote Host	UDID Hostname / Cookie Lifetime	Reverse DNS	GeoIP Location	Netblock Owner
ABC News	UDID		wdgwnewabcnewsiphoneapp.112.2o7.net	*.112.2o7.net	Dublin, CA	Omniture
ABC News	Cookie	abcnews.go.com	Expires: 20 years			
AlJazeera	UDID	216.74.41.4	data.flurry.com			
AlJazeera	UDID	70.32.132.54	mm.admob.com			
AlJazeera	UDID	209.170.118.123	r.admob.com			
AlJazeera	UDID	173.194.35.148	ad.doubleclick.net			
AlJazeera	UDID	70.32.130.40	clk2.vip.sc9.admob.com			
BBC	UDID	66.235.132.232	bbc.112.2o7.net	*.112.2o7.net	Dublin, CA	Omniture
BBC	Cookie	www.bbc.co.uk	Expires: 4 years			
CBS News	UDID	174.129.199.130	ads.admarvel.com	Amazon EC2	Breezewood, PA	Amazon.com
CBS News	UDID	216.74.41.4	data.flurry.com	441gift.com	Denver, CO	WCP/32POINTS
CBS News	UDID	72.5.61.135	cbsnews.ian.dw2.treemo.com	None	Seattle, WA	Internap / Hyperboy, LLC
CBS News	UDID	184.73.92.77	184.73.92.77	Amazon EC2	Seattle, WA	Amazon.com
CBS News	Cookie	ads.admarvel.com	1 year			
CBS News	Cookie	view.atdmt.com	18 months	calls itself a "Tracking Agent"		
CNET	UDID	174.129.226.20	ads.admarvel.com	Amazon EC2	Seattle, WA	Amazon.com
CNET	UDID	216.74.41.4	data.flurry.com	441gift.com	Denver, CO	WCP/32POINTS
CNET	UDID	184.73.56.203	184.73.56.203	Amazon EC2	Seattle, WA	Amazon.com
CNET	Cookie	ads.admarvel.com	1 year			
CNET	Cookie	cbsnews.treemo.com	1 year			
CNET	Cookie	view.atdmt.com	2 years			
Fox News	UDID	74.86.76.66	a.medialytics.com	74.86.76.66-static.reverse.softlayer.com	Dallas, TX	SoftLayer Technologies
Fox News	Cookie	core.ringleaderdigital.com	17 months			
Huffington Post	No UDID or Persistent Cookies					
MSNBC	Cookie	openx.zumobi.net	Expires: 1 year			
NPR	UDID	74.86.76.66	t.medialytics.com	74.86.76.66-static.reverse.softlayer.com	Dallas, TX	SoftLayer Technologies
NPR	Cookie	www.npr.org	Note: Cookie is not set by server			
NY Times	UDID	216.74.41.4	data.flurry.com	441gift.com	Denver, CO	WCP/32POINTS
NY Times	Cookie	iphone.nytimes.com	not set by server			
NY Times	Cookie	www.nytimes.com	1 year			
USA Today	"UserID"					