The GAB'er

The Newsletter of the Greater Albany Apple Byters

Volume 27, Number 9 - May 2011

New Thunderbolt-Equipped iMacs

On Tuesday, Apple announced a new generation of iMac models, running at speeds up to 3.4 GHz and powered by the next generation of Intel Core i5 and Core i7 processors. The models also build in support for the new Thunderbolt high-speed peripheral connection interface that debuted in Apple's MacBook Pro line earlier this year.

The watchword of the new model is "performance," thanks to improvements in the processor line, graphics architecture, and Thunderbolt ports.

In terms of processors, Apple has shifted to Intel's second-generation Core technology—codenamed "Sandy Bridge"—for the iMac line. "What Intel has done is very tightly engineer the processor, the graphics, the cache, and the memory controller on a single die," said Apple's David

Continued on page 11.

Coordinator's Corner

by John Buckley

When it comes to working with multiple computers and other electronic devices, one of the real problems is keeping everything organized. That is where MobileMe comes into play.

This month we will look at MobileMe and with the possibility of it becoming a free service, Mac users may want to give it another look to see if they may want to use it in the near future. This was what we were going to do last month when I became ill.

In addition we will discuss what we will be doing for our June meeting. This has usually be a social event where we go out to dinner. Therefore, you should bring ideas about possible locations if we are to continue this tradition.

As usual, check our website for the most current GAAB information. You will find a map and aerial photograph showing how to get to the meeting location.

In addition, we take a look at what is now available from Apple including the new Snow Leopard tips and Apple announcements over the past month.

Continued on page 10.

Next GAAB Meeting
May 11, 2011

MobileMe

7:00 p.m.

St. Mary's Hospital,
Troy, NY

Featured in this Issue

Serving the Apple Computer User Community Since May 1984

The Greater Albany Apple Byters is an Apple Computer User Group. Meetings are held the second Wednesday of each month (except July and August) in Room 212 of Troy High School, located on Burdett Avenue, Troy, NY.

Annual membership fee is $10.00. Membership privileges include this newsletter, access to a large public domain software and video/audio tape library, local vendor discounts, special interest groups, and other special offers.

The views expressed herein are the sole responsibility of each author, and do not necessarily represent the views of the Greater Albany Apple Byters.

Note: Trademarks used in this newsletter are recognized as trademarks of the representative companies.

Officers & Special Interest Group Leaders

Program Coordinator
John Buckley
272-7128

Membership Director
Cecilia MacDonald
872-0823

Treasurer
Cecilia MacDonald
872-0823

Public Domain Librarian
Bill Shuff
393-9753

Newsletter Editor
Roger Mazula
466-7492

Education SIG
John Buckley
272-7128

Internet SIG
Lou Wozniak
465-2873

Apple Ambassador

by John Buckley

Is Apple Tracking You?

The big rage over Apple this past month has been the fact that iPhones, iPod Touches, and iPads have be keeping tabs on where they have been using information from cell phone towers and WiFi locations you may have passed through. While this is technically not a Mac issue, it is something we should be aware of as technology takes more and more of our personal information and makes it public. The following is a press release from Apple concerning the issue.

Apple Q&A on Location Data

Apple would like to respond to the questions we have recently received about the gathering and use of location information by our devices.

1. Why is Apple tracking the location of my iPhone?

Apple is not tracking the location of your iPhone. Apple has never done so and has no plans to ever do so.

2. Then why is everyone so concerned about this?

Providing mobile users with fast and accurate location information while preserving their security and privacy has raised some very complex technical issues which are hard to communicate in a soundbite. Users are confused, partly because the creators of this new technology (including Apple) have not provided enough education about these issues to date.

3. Why is my iPhone logging my location?

The iPhone is not logging your location. Rather, it's maintaining a database of Wi-Fi hotspots and cell towers around your current location, some of which may be located more than one hundred miles away from your iPhone, to help your iPhone rapidly and accurately calculate its location when requested. Calculating a phone's location using just GPS satellite data can take up to several minutes. iPhone

Continued on page 7.

Internet SIG

Control What's Online About You

by Kim Komando

Your age and marital status. Your home's value and your estimated annual income. Intimate details of your social life. Stalkers, nosy neighbors and potential employers can find this data and more. All it takes is a quick Web search.

As more of your life moves online, you need to manage your online reputation. Foil stalkers and snoops by limiting the available information. At the same time, you want to present your best side to employers and business associates.

This isn't easy. With a little know-how and persistence, you can do it.

Remove unflattering and sensitive information

The first step is to see what information is available. Start with Google, Yahoo and Bing. Search for variations of your name; if you have a common name, add qualifiers like your city. Results near the top matter the most. However, unflattering details may appear on subsequent pages. Make a list of content to change or remove. Make a second list of content to promote.

Next, list online accounts you no longer use. Old dating profiles and social-networking pages can come back to haunt you. Privacy rules for these sites can also change. Close old accounts.

Your data also appears on people search sites and online databases. This is trickier to remove and often reveals sensitive financial details. These sites pull data from public records; they'll sell a complete file on you to anyone with cash. Each has different removal instructions; you must request removal from each site individually.

Requesting removal won't necessarily keep your data safe. Many sites make it difficult or impossible to remove data. Because this information comes from public records, it may reappear later.

Click here for a list of data brokers and people search sites. I've also got removal instructions for big sites like Spokeo and MyLife.

You should also review your Facebook account. Limit sensitive information like your full birth date and home address to close friends and family. Remove or hide embarrassing posts.

There's a chance that unflattering information may appear on other sites. This can prove difficult to remove, particularly if it is factually correct. Your best bet is to write the site owner a polite letter making your case. Be sure to highlight any inaccuracies.

If the posts seem intentionally malicious, contact Google. In some cases, it removes links from searches. You may also consider contacting an attorney.

Promote the positive

It can take weeks to clean up your online reputation. Simply trying to remove data may not do enough. You may need to create content to push down unflattering search results. This gives you the ability to control what people see.

Several things will help. Create a profile on Linked In highlighting your professional accomplishments. Create a Google Profile. Use it to direct people to information you want them to see. Link to positive stories about you. Include links to other carefully selected sites.

Start a free blog with Blogger or WordPress. Cover your personal or professional interests and showcase your abilities. Others online will likely have your same name. This can be potentially embarrassing. In that case, create a post with links to others that share your name. It's a direct way to distinguish yourself.

Finally, you may not be able to control your online reputation yourself. Fortunately, there are companies that can help. Reputation.com and Reputation Hawk specialize in online reputation management. Prices start around $100 and can run into the thousands.

Education SIG

Confronting Cyberbullying

by Peter Levy, The Journal

Experts say that schools need to stop worrying about external internet predators and take on the threat within: cyberbullying

In the late 1990s and early 2000s, as schools first started getting widespread access to the internet, many administrators saw the potential in this new technology, but also huge risks and liabilities. While billions were being spent on hardware and connectivity, the mainstream media was fueling parental fears with stories of online predators waiting at every exit of the new information superhighway. The response from many schools was initially to teach internet safety in terms of protection from the two P's: predators and pornography. With funding coming from the Department of Justice, teacher training was conducted by law enforcement personnel and student assemblies often included uniformed police officers. At the same time, numerous well-meaning nonprofits appeared, seeking to help educators communicate with parents and students, but still through a lens of fear and protection.

Many experts now believe this was very much the wrong approach. "We missed the boat by concentrating on internet predators," says Patti Agatston, a nationally recognized counselor and cofounder of Cyberbullyhelp.com. Larry Magid, codirector of Connect Safely.org concurs that "predation is statistically so unlikely that it's not where we should be putting our resources."

The focus today, Agatston and Magid agree, should be on empowering kids to be good digital citizens. Groups such as Common Sense Media have in recent years helped to reframe their discussion in terms of the skills students need to live successful, technology-rich 21st century lives. Acquiring these proficiencies requires a positive and more holistic approach: how to protect personal information, interact in social forums, deal with cyberbullying, and critically judge online information are all among these vital skills. By focusing on how schools do want kids to behave online rather than on how we don't want them to behave, "We let them assume responsibility for their own learning and their own online experience," says Linda Burch, Common Sense Media's chief education and strategy officer.

Elevating the Issue

Common Sense Media, along with groups such as Media Awareness Network, BrainPop, Learning.com, and Web Wise Kids all offer a breadth of resources to address these issues. While these organizations strongly encourage administrators to institute the full range of digital literacy curricula, the combination of students with smartphones, the expanded usage of social networking sites, and high-profile media coverage of recent cyberbullying tragedies has elevated the issue of cyberbullying to the top of many administrators' worry lists.

"Bullying and cyberbullying have a lot in common, but in many ways, cyberbullying is even more pernicious," says Anne Schreiber, vice president of education content at Common Sense Media. Schreiber points out that the cyberbully doesn't see his or her victim, which makes it easier to have less empathy than in a face-to-face interaction. What's more, anything written in a text or online chat or on a social networking site can be forwarded to any number of people with just a few clicks, escalating the problem beyond, say, a corner of the school cafeteria.

Schreiber recounts a recent cyberbullying incident that began with a series of hostile text messages at school in the morning. By the afternoon, a fight had broken out between friends of the bully and friends of the victim--the harsh words were forwarded over and over until the whole school was involved. "Because the bullying spread so quickly through viral texting, there was no time for the individuals to cool off and think about how to behave rationally or ethically," Schreiber notes.

Administrators can't shrug off issues of cyberbullying by arguing that the bulk of the issues happen with kids outside of school or that they simply don't have time in the school day. Agatston, who is the coauthor of Cyber Bullying: Bullying in the Digital Age, says that although she appreciates that school leaders are pressed for time to confront these issues, "if they can see the link between academic achievement and bullying, they'll see that it's well worth the time." Agatston's research suggests that addressing cyberbullying in school improves attendance as well as students' focus on their schoolwork.

What's needed, ConnectSafely's Magid contends, "is a sustained campaign where bullying is as 'out' as racism or smoking." To accomplish this, experts suggest a unified and comprehensive approach, which requires that schools integrate cyberbullying education into their curriculum and adequately provide for teacher training.

Agatston says that schools must cast a broad net in terms of who they involve in the discussion of safe online usage. "Within schools we need to move from the idea of anti-bullying being the responsibility of the school counselor to being the responsibility of the whole school community, which includes parents," she says.

Staff Training Is Key

If school leaders are going to engage more members of the school community, recent data suggests that much work still needs to be done with classroom teachers. According to a 2010 survey from the National Cyber Security Alliance, just 50 percent of teachers who participated in the study felt prepared to discuss cyberbullying. Over three quarters of teachers surveyed spent less than six hours on any type of professional development education related to cyberethics, cybersafety, and cybersecurity within the last 12 months.

Many states around the country, including Massachusetts, Maine, and Rhode Island, as well as districts such as Kentucky's Pike County Schools, have demonstrated that programs that educate their schools and, in some cases, their entire communities about the responsible use of technology can be effective. In Pike County, for example, the district was struggling in 2007 with extensive violations of its Acceptable Use Policy (AUP). After it implemented on-site professional development to support digital citizenship, the impact has been substantial. Since 2009, only two AUP violations have been recorded.

Burch says she's optimistic about schools' abilities to substantially curb issues of cyberbullying, pointing out that more than 12,000 schools have already registered to use Common Sense Media's curriculum. Burch also sees a range of positive signs that both government and media companies are also focusing on the issue. In March, the White House launched StopBullying.gov to offer resources for students, parents, and educators on how to detect, intervene in, follow up on, and prevent bullying, including cyberbullying. The site, which was launched in concert with a White House Conference on Bullying Prevention, serves to shine a national spotlight on the issue.

On the media side, MTV recently launched its "A Thin Line" online campaign, which offers a brief user quiz followed by short, engaging videos that each highlight the message that there's "a thin line" between what may begin as a harmless joke and something that could end up having a serious impact on the person playing the joke or another human being. Nicelodeon recently announced that it will be creating a series of public service announcements around the issue of internet safety and will embed themes of healthy technology usage into such popular shows as iCarly. Cable in the Classroom, the public service arm of the cable industry, has numerous educational resources on digital citizenship, including cyberbullying.

Facebook also announced that it would be making changes to how users report inappropriate activity. A new feature, dubbed "social reporting," will give users new options for reporting offensive photos or Wall posts. For example, kids can now notify a trusted source, such as a parent or teacher, of foul play. In addition, when users click "Report" on a photo, a pop-up window will appear asking if the photo is about the user. If it is, the user can select "I don't like this photo" or "This photo is harassing or bullying me."

Best Practices

Back at school, many districts are in need of expanding or revising their policies and procedures around dealing with these important 21st century issues. The best digital citizenship programs have a number of features in common, which administrators can consider as best practices. Agatston offers the following guidelines:

Assess cyberbullying: Effective bullying prevention programs begin with an assessment of the problem in your school or district.

Develop clear policies: Policies should address both on-campus and off-campus acts that have or could have a substantial disruption on student learning or safety.

Provide staff training: Just as staff training is needed to adequately address bullying behavior and encourage positive bystander behavior (and in a broader sense, "citizenship"), training on preventing and responding to

cyberbullying, as well as the broader topic of encouraging positive digital citizenship, is a necessary part of any digital citizenship program.

Spend class time on the topic of cyberbullying and positive digital citizenship: Classroom discussions should be part of the regularly held discussions on bullying and cover such topics as defining cyberbullying; school policies and rules regarding cyberbullying; how to report cyberbullying behavior; how to best respond to cyberbullying behavior; and the bystander role as it applies to cyberbullying.

Teach students online "netiquette," safe use of social media, and how to monitor their online reputation: These vital social skills also have an impact on job preparedness, as social technology is increasingly being incorporated into most career paths. Lessons can be infused throughout the curriculum where appropriate. Discussions can take place when using technology in the classroom as well as when addressing career and college guidance.

Train and utilize student mentors: Effective prevention programming includes incorporating youth leadership, particularly to address school climate issues. Making use of student leadership sends a strong message to other youth and also recognizes that the peer group often has more legitimacy than the teacher in addressing social issues.

Form parent/community/school partnerships: Everyone has a role to play in encouraging positive digital citizenship. Schools need to partner with parents and community organizations in making sure that there is a consistent message about the responsible and ethical use of technology.

Ultimately, school districts should work to foster a school environment where young people are free to express themselves and their identity online, but do it in a safe, thoughtful, and respectful manner. Burch says this comes by empowering students to see that "we all have roles and responsibility to ourselves, to our friends and family, and to the community we belong to, whether that's a school or an organization or an online community." Burch believes that kids respond well when leaders cast an affirming and inclusive frame around the issue of digital citizenship. "This is their world," she says. "They want to make it a positive one."

Mac vs. PC: The Stereotypes May Be True

by Brandon Griggs, CNN

Remember those Apple ads that cast the Mac as a 20-something, self-satisfied hipster while the PC was portrayed by an older, square-looking guy in a brown suit?

Well, those characterizations, unfair as they may be, appear to have some truth to them.

An unscientific survey by Hunch, a site that makes recommendations based on detailed user preferences, found that Mac users tend to be younger, more liberal, more fashion-conscious and more likely to live in cities than people who prefer PCs.

Of the 388,000 Hunch users who responded to a question about computer loyalty, 52% identified themselves as PC people as opposed to 25% who said they are Mac devotees. Hunch then cross-referenced those responses with answers to other questions to draw cultural distinctions between the rival Mac and PC camps.

The results suggest Mac users can be seen, depending on your perspective, as bolder and more creative -- or elitist and more pretentious.

The report found that 67% of Mac users have a college or advanced degree, as opposed to 54% of PC users. Mac loyalists are 80% more likely than PC users to be vegetarians, and, unlike PC fans, would rather ride a Vespa scooter than a Harley.

PC users' tastes trend towards casual clothes, tunafish sandwiches, white wine, Hollywood movies, USA Today and Pepsi. Mac users prefer designer or vintage duds, hummus, red wine, indie films, The New York Times and (we're not making this up) San Pellegrino Limonata.

Mac users also are more likely to describe themselves as computer-savvy and "early adopters." PC users tend to describe themselves as better at math and less likely to throw frequent parties.

"I fit the typical Mac user on every count. Guess I'm not as unique as I thought. Depressing," wrote one commenter on Hunch's blog.

Since Hunch's first survey of Mac vs. PC users in November 2009, Apple has ridden the success of such high-profile products as the iPad and iPhone 4 to become the world's most highly valued tech company. Despite that hot streak, Hunch found that slightly more people in its new report -- 52%, up from 50% a year and a half ago -- now identify themselves as PC users.

Apple Ambassador

Continued from page 2.

can reduce this time to just a few seconds by using Wi-Fi hotspot and cell tower data to quickly find GPS satellites, and even triangulate its location using just Wi-Fi hotspot and cell tower data when GPS is not available (such as indoors or in basements). These calculations are performed live on the iPhone using a crowd-sourced database of Wi-Fi hotspot and cell tower data that is generated by tens of millions of iPhones sending the geo-tagged locations of nearby Wi-Fi hotspots and cell towers in an anonymous and encrypted form to Apple.

4. Is this crowd-sourced database stored on the iPhone?

The entire crowd-sourced database is too big to store on an iPhone, so we download an appropriate subset (cache) onto each iPhone. This cache is protected but not encrypted, and is backed up in iTunes whenever you back up your iPhone. The backup is encrypted or not, depending on the user settings in iTunes. The location data that researchers are seeing on the iPhone is not the past or present location of the iPhone, but rather the locations of Wi-Fi hotspots and cell towers surrounding the iPhone's location, which can be more than one hundred miles away from the iPhone. We plan to cease backing up this cache in a software update coming soon (see Software Update section below).

5. Can Apple locate me based on my geo-tagged Wi-Fi hotspot and cell tower data?

No. This data is sent to Apple in an anonymous and encrypted form. Apple cannot identify the source of this data.

6. People have identified up to a year's worth of location data being stored on the iPhone. Why does my iPhone need so much data in order to assist it in finding my location today?

This data is not the iPhone's location data—it is a subset (cache) of the crowd-sourced Wi-Fi hotspot and cell tower database which is downloaded from Apple into the iPhone to assist the iPhone in rapidly and accurately calculating location. The reason the iPhone stores so much data is a bug we uncovered and plan to fix shortly (see Software Update section below). We don't think the iPhone needs to store more than seven days of this data.

7. When I turn off Location Services, why does my iPhone sometimes continue updating its Wi-Fi and cell tower data from Apple's crowd-sourced database?

It shouldn't. This is a bug, which we plan to fix shortly (see Software Update section below).

8. What other location data is Apple collecting from the iPhone besides crowd-sourced Wi-Fi hotspot and cell tower data?

Apple is now collecting anonymous traffic data to build a crowd-sourced traffic database with the goal of providing iPhone users an improved traffic service in the next couple of years.

9. Does Apple currently provide any data collected from iPhones to third parties?

We provide anonymous crash logs from users that have opted in to third-party developers to help them debug their apps. Our iAds advertising system can use location as a factor in targeting ads. Location is not shared with any third party or ad unless the user explicitly approves giving the current location to the current ad (for example, to request the ad locate the Target store nearest them).

10. Does Apple believe that personal information security and privacy are important?

Yes, we strongly do. For example, iPhone was the first to ask users to give their permission for each and every app that wanted to use location. Apple will continue to be one of the leaders in strengthening personal information security and privacy.

Software Update

Sometime in the next few weeks Apple will release a free iOS software update that:

- reduces the size of the crowd-sourced Wi-Fi hotspot and cell tower database cached on the iPhone,
- ceases backing up this cache, and
- deletes this cache entirely when Location Services is turned off.

As promised last week, Apple will reportedly fix location-tracking software on the iPhone and other devices in an update to its iOS mobile operating system in the next few weeks.

Apple will release iOS version 4.3.3 "within the next two weeks, possibly sooner," BGR.com reported Monday, citing a company source.

The update for iPhones and iPad tablets will address several location-tracking issues that came to light in April when two researchers publicized the existence of an unencrypted, hidden file on iPhones that stores location data taken from nearby cell towers and Wi-Fi hotspots. The cached data is also timestamped, backed up on iTunes and although

associated with Apple's Location Services, cannot be shut off by users when they opted out of the service.

The iOS 4.3.3 update promises to end the backing up of the location database when devices are synched to iTunes, reduce the size of the cached data file and delete the database when users turn off Location Services, according to BGR.com.

There will also be some improvements in 4.3.3 that aren't related to location tracking, including a boost to battery life and fixes for bugs in the iPod Touch.

The last piece of Apple's PR nightmare over what it calls location-tracking "bugs"—the lack of encryption for the location data cache—won't be addressed until the "next major iOS software release," the company stated last week.

The following article from The Next Web Family provides further information about this issue and how to turn the tracking off.

Your iPhone has been storing general data about it's location since at least last September. It has been doing this in an unencrypted data file that is stored on your phone and in your backup files on your computer. That file is easily accessible to anyone with physical access to your phone or your computer.

That information used to be in the inaccessible system partition of the iPhone previous to the release of iOS 4.0. This information was not contained in iPhone backups and was ostensibly accessible only to Apple or people that had Jailbroken iPhones.

Now, the information resides in a section of your iPhone's memory that is contained in iPhone backups and that is easily accessible to programs like the iPhone Tracker. Both GSM and CDMA iPhones record this location data.

Those are the facts. Anything else is conjecture or based off of unsubstantiated inside information.

Where is the information stored?

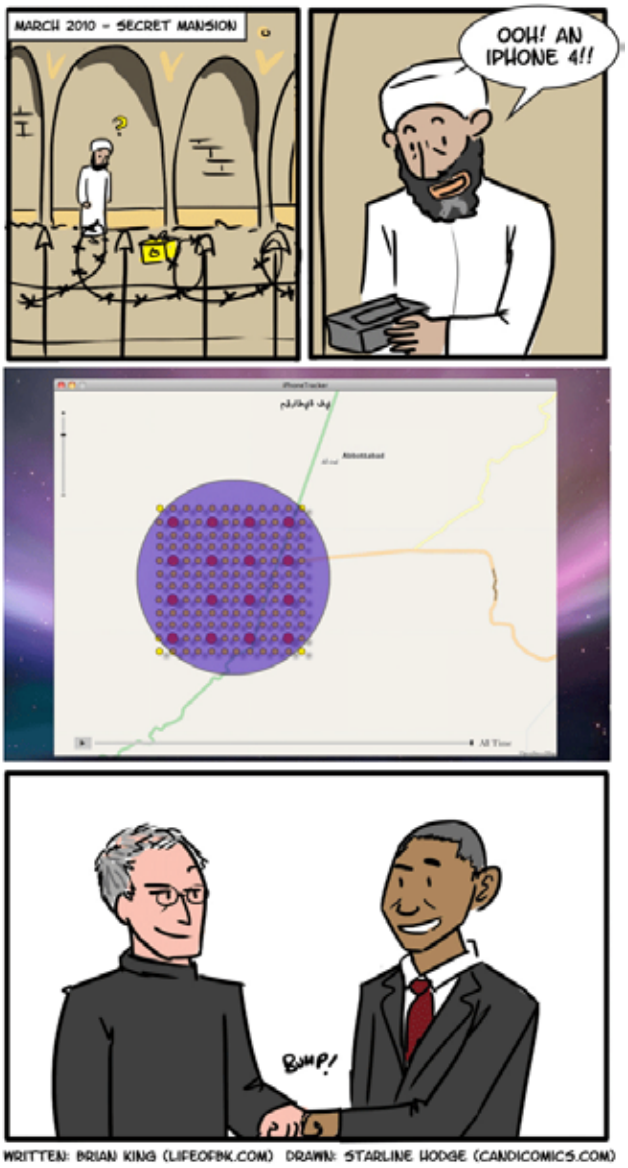
The fact that the iPhone was collecting and keeping this data was originally discovered last September by iPhone security expert Alex Levinson. The file, called *consolidated.db* is stored on the User partition within the iPhone's file structure, making it accessible and allowing it to be contained in iPhone backups.

The file where this data used to be collected pre-iOS 4.0, was called *h-cells.plist* and it was located in the system partition and, while still accessible with enough effort, was much harder to get to and was not contained in backups.

Why was the data moved?

Some conjectures have been made that Apple moved this data in order for it to be easier for Apple itself or government officials to track iPhone users.

The fact of the matter is that the data was most likely moved for a much less nefarious reason. Developers needed access to the data to use in Multitasking and background location APIs. With the data behind the system partition, developers would not have been able to take advantage of cell tower triangulation in addition to GPS location to determine the iPhone's location.



Why is it being gathered?

There are two main possibilities for the data collection. First, it's obvious that making the data available to developers who are using location based services in their apps is necessary.

If you've ever used Google Maps and had the blue dot pop up a couple of blocks away from where you are with a large blue circle around it, that location was obtained using the same data that's stored in this file. Your exact location is then determined by the GPS radio in your phone. If you're indoors or have the GPS turned off, this data is used to approximate your location for apps that need it.

The other main reason that it could be being collected is that Apple is gathering information on the distance between, strength and positioning of cellular towers. A recent update to the iPhone Location app has determined that the information is recorded on both CDMA and GSM phones.

We've contacted Apple to confirm the exact reason that it's being gathered but have not heard back from them yet. If we receive more information we will let you know immediately.

Why is it being kept?

This is the question that many who understand what we've discussed above are asking. If your iPhone only needs it for basic positioning, then why is the data being stored long term?

One theory has been posed by John Gruber of Daring Fireball. I don't have a definitive answer, but my little-birdie-informed understanding is that consolidated.db acts as a cache for location data, and that historical data should be getting culled but isn't, either due to a bug or, more likely, an oversight.

The supposition here is that Apple always intended for the data to be erased a short time after it was recorded. After it was used for whatever positioning purposes that it was gathered for, it would be erased from the log file. Most likely this would happen on a revolving time-frame. Once data passed out of the time frame of usefulness, it would be deleted from the end of the database.

The answer as to why it is being kept can only be answered by Apple at this point, another item that we have reached out to them for comment on.

Is the information being sent?

Here is the important question. Apple has already acknowledged publicly that they do record and transmit data about cell phone towers in a letter to congress. In that letter, prompted by an inquiry from Congressmen Edward J. Markey and Joe Barton, Apple explains that they do gather this data and that it is transmitted but that it is done so in an encrypted packet.

Whether or not the data is sent encrypted remains to be seen, but the file is certainly not encrypted on your hard drive or the iPhone itself.

Although there was never any official confirmation of this, there is a strong possibility that the mysterious data transmissions many users have seen their iPhones performing in the wee hours of the night do, in fact, contain this location tracking information. The file size of the consolidated.db file and the amount of data being transmitted are similar enough to posit a possible link.

Can I stop it from being recorded?

Currently the only way to stop it from being recorded is to jailbreak your iPhone and use a jailbreak app written specifically for the purpose. Turning off location services will not disable the recording of this data as it's considered diagnostic information.

You can also encrypt your iPhone backups which will protect the file from anyone attempting to access it on your machine. Doing this will not protect the file on your phone itself however.

In order for the file itself to be protected from access it would either need to be moved back to the system partition, where it is still possible to find but much more difficult for the average user, or encrypted by Apple on-device.

Should I be worried?

At worst the gathering of location data from GSM and CDMA cellular towers should be of mild concern to anyone who is in danger of their iPhone or computer being accessed by people that could be in a position to use your location to harm you.

This cross-section of people should be fairly limited.

That doesn't mean that Apple shouldn't have to do something about this file though. It's unnecessary to have all of your movements for the past 8 months just sitting on your phone. A software update that either aggressively culled the file of old data or made it more secure will most likely be incoming.

We will be sure to inform you immediately if Apple responds to our inquiries regarding the iPhone recording your location and whether or not it is in fact being transmitted.

Program Coordinator

Continued from page 1.

To find out what's happening, GAAB is the place to be. So be sure to be at our April meeting and every meeting to find out the best information about the Mac.

The April meeting will be held at St. Mary's Hospital in the Leonard Board Room on Wednesday, May 11, 2011. The meeting will begin at 7 p.m. St. Mary's Hospital is located at 1300 Massachusetts Avenue in Troy NY.

However, the best route to take from the Northway is the following:

1. Merge onto NY-7 East from the Northway.
2. Follow Route 7 to Troy where it becomes Hoosick Street.
3. Turn left on Oakwood Avenue (10 Street/NY-40) which is the first light after the bridge and bare right.
4. Turn right on Sausse Avenue. Turn left onto Lindenwood Court. When you come to the first entrance to the hospital parking lot, turn left and park.

Any Questions?

New iMacs

Continued from page 1.

Moody, vice president of hardware product marketing. Moody said this accelerates data transfer between processor components, resulting in some impressive performance gains.

In addition, the processor architecture upgrade has enabled a transition to quad-core processor configurations across the iMac line—in comparison, the previous iMac line had only a single quad-core configuration on the highest-performance model.

"What we see as a result of moving from dual-core to quad-core and old architecture to new architecture is 70 percent faster performance than the old models," said Apple's Moody. "Even in the top-end, moving from the old quad-core configuration to the new quad-core configuration has seen 30 percent faster performance."

Processors aren't the only place that the iMac has seen a significant boost; the desktop line now sports the latest generation of AMD Radeon HD discrete graphics processors. The high-end Radeon HD 6790M boasts 1.3 Teraflops of performance and is up to 80 percent faster than the previous generation. Moody described the technology as "Mac Pro-class graphics" and said it's the "first time we have the same level of performance in the iMac that you'd have in a Mac Pro." The gains aren't limited to high-end either; even the entry-level version's Radeon HD 6750M graphics processor clocks in at three times faster than the previous configuration.

For external connectivity, the new iMacs boast the same Thunderbolt ports introduced in Apple's new MacBook Pro line released in February. Co-developed with Intel, Thunderbolt offers two bi-directional channels that can transfer data at up to 10Gbps each—12 times faster than the theoretical maximum of FireWire 800. The technology is based on the PCI Express protocol that most Macs use for internal I/O, but via adapters it can support pretty much any other type of connectivity protocol, including FireWire, USB, and Gigabit Ethernet.

The smaller iMac sports a single Thunderbolt port while the larger version includes two—Moody confirmed that those ports are independent as well, meaning that users essentially have four 10Gbps channels. That allows, for the first time, the 27-inch iMac to drive two external displays—and that's in addition to other high-speed peripherals. Moody also said that the adoption of Thunderbolt is progressing, with several vendors announcing plans for compatible peripherals at the NAB show last month.

As with the MacBook Pro refresh also earlier this year, the iMac line also now has a FaceTime HD camera for video conferencing. The camera supports 720p high-definition video in a 16 by 9 widescreen format, and supports a wider viewing angle to make it easier for multiple people to get in the picture. High-definition video calls are only supported between Macs with a FaceTime HD camera, such as the iMac and MacBook Pros—calls with other Macs or iOS devices are limited to standard definition.

The new machine comes in four basic configurations: two 21.5-inch models with a 2.5GHz Quad-Core Intel Core i5 and 2.7GHz Quad-Core Intel Core i5 processor respectively, and two 27-inch models with a 2.7GHz Quad-Core Intel Core i5 and 3.1GHz Quad-Core Intel i5. Apple is also offering build-to-order Web-only options to bump the 21.5-inch model to a 2.8GHz quad-core Intel Core i7, and the 27-inch model to a 3.4GHz Intel Core i7; the i7 processor upgrades add $200 to the cost.

The low-end 21.5-inch model sports a 500GB hard drive and an AMD Radeon HD 6750M with 512MB of video RAM, while the more powerful 21.5-inch configuration has a 1TB hard drive and an AMD Radeon HD 6770M with 512MB of video RAM. Both versions feature a 1920 by 1080 pixel display and 4GB of memory. They retail for $1,199 and $1,499 respectively.

Both of the 27-inch models sport a 1TB hard drive, 4GB of RAM, and a 2560 by 1440 pixel display. The 2.7GHz model has an AMD Radeon HD 6770M with 512MB of video RAM, while the 3.1GHz model has an AMD Radeon HD 6970M with 1GB of video RAM. They cost $1,699 and $1,999 respectively.

Additional build-to-order options include 2TB hard drives, an additional 256GB solid-state drive instead of or alongside the main drive, and up to 16GB of DDR3 memory. Customers can choose a Magic Mouse, a Magic Trackpad, or both with their order.

The new iMac also meets the Energy Star 5.2 requirements and achieves EPEAT Gold rating, according to Apple. The computer is built with components that are free of mercury, arsenic, PVC, and brominated flame retardants.

GAAB Internet Addresses

Names	E-Mail Addresses
Aaron Ambrosino	aambrosi@mac.com
Gary Blizzard	gmblizzard@aol.com
Mark Bogossian	mark@castlecomp.com
Steve Bradley	ssbradley@adelphia.net
John Buckley	jbuckley@nycap.rr.com
Sheldon Carnes	sheldoncarnes@hotmail.com
Tina Cook	twonotrump@nycap.rr.com
Anthony Eldering	tonye11@verizon.net
Trudy Ellis	TE52@earthlink.net
Lilajane Frascarelli	afrascar@nycap.rr.com
Les Goldstein	lgoldst1@nycap.rr.com
Richard Hester	hesterfp@capital.net
Ottmar Klaas	ottmar.klaas@gmail.com
Michael LaFrank	mlafrank@nycap.rr.com
Thomas Levanduski	msglevnduski@aol.com
Cecilia MacDonald	cecilia@midtel.net
Mike Mannarino	rfd230@nycap.rr.com
Roger Mazula	aluzam@aol.com
Brendan O'Hara	bohara1@nycap.rr.com
Eric/Lee Rieker	Erieker@aol.com
AbdurRahman Rozell	aryr100@gmail.com
Judith Schwartz	jfschwartz2@earthlink.net
Saul Seinberg	saul.seinberg@gmail.com
Bill Shuff	wjshuff@earthlink.net
Shelly Weiner	olliedawg@yahoo.com
Lou Wozniak	louw@nycap.rr.com

To start or renew your GAAB membership, see Cecilia MacDonald or send your fees payable to her at the following address:

Cecilia MacDonald
260 Sever Road
Delanson, NY 12053

Visit GAAB on the Internet at http://www.applebyters.com