July 2012
Geoff Huston

All Your Packets Belong to Us

What Happened…

On the 18th June, it was reported on an Australian users' forum, Whirlpool, that whenever a Telstra mobile data service user contacted a web site, then some 250ms later the same web site URL was fetched from a different source address. It appeared that somehow this third party was stalking the mobile data user, visiting all the same web sites as the user, in every case shortly after the user. (http://forums.whirlpool.net.au/forum-replies.cfm?t=1935438)

This third party was reported to be on the IP addresses 50.57.104.33 and 50.57.190.97. These addresses are used by *Slicehost*, who appears to be a hosting service provider located in San Antonio, Texas in the US.

Other users reported on the same behaviour, and it quickly became evident that this was a more general behaviour that had been quietly introduced by this national carrier without any form of notice to their users. The observed behaviour was that all URLs used by end users of their mobile network, whether private or public, were being passed across to this US-based third party, who in turn were repeating the original access call to the visited URL, if the URL was a novel URL. There was some speculation in the forum on the particular motives were driving Telstra to stalk its users in this manner, and some speculation that Telstra was attempting to monetize its user's browsing behaviour by on-selling this user behaviour data to a foreign third party.

> Perhaps we are just being too sensitive about privacy. On the other hand maybe we are not sensitive enough, as it is certainly the case that there are incredibly strong business cases that justify spending large money in order to peek over the shoulders of users and intrude into their activities, not only to understand their behaviour but to influence their future behaviours. If anyone is in doubt about the true value of user behaviour data and how to influence future behaviour, then perhaps a read through New York Times article on "How Companies Learn Your Secrets" may be useful at this point. (http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html)

In response to an accusation of unethical behaviour on the part of Telstra, a local industry publication, SC Magazine, reported the following:

> "But in a short statement, Telstra's senior media boss Craig Middleton said the company's wireless network management assured that "there is nothing untoward in what the Whirlpool member has observed - it is a normal network operation"."
> [http://www.scmagazine.com.au/News/305928,telstra-says-its-not-spying-on-users.aspx]

To attempt to brush off such accusations of invasion of a user's reasonable expectations of privacy in their use of a public carriage network in such a cavalier and off-hand manner was a less than brilliant move by company executive who was purportedly the head of their media unit. This close stalking of user behaviour is anything but "normal network operation." Perhaps the best way to fuel further speculation about dark motives and conspiracies is to attempt to brush it off with an obvious lie. And that is precisely what Telstra did.

At this point the speculation was that the observed user stalking behaviour was the result of Telstra selling off a real time feed of each user's browsing history to a US-based marketing company. This theory gathered a lot of credibility in discussion forums in the space of a few hours.

It was also apparent that this was not something that individual users could opt out of. It appeared that this was a behaviour that appeared to be imposed on the users' browsing behaviour in all of Telstra's mobile data services.

A few days later, on the 26th June, it was reported that:

> "Telstra has confirmed it is tracking websites visited by its mobile users in the lead up to a launch of a new web filtering solution.
>
> Days after suspicions of Telstra's networking monitoring activity was first aroused, the telco has revealed it captures web addresses visited by millions of subscribers on its Next G network.
>
> The addresses are compared to a blacklist of criminal sites curated by web filtering company Netsweeper, and held both in Australia and the US.
> [http://www.scmagazine.com.au/News/306441,telstra-tracks-users-to-build-web-filter.aspx]

And at the same time Telstra rushed out a new set of terms and conditions for its data services with a new feature called "Smart Controls," complete with a collection of spelling errors in the revised document that pointed to a lack of proofreading and perhaps certain level of haste and possibly panic on the part of Telstra.

At this point things became political. Greens Senator Scott Ludlam was reported as saying that sending even anonymised traffic offshore could have serious privacy implications. He was reported to have said:

> "It is potentially problematic. Anything in the US is subject to the Patriot Act, even if the data is anonymised, or sent as batches."

(The US Patriot Act, introduced in 2001, grants the US Government wide-ranging powers to access any user data stored within the US for intelligence purposes.)

The mainstream press also picked up the story, and Telstra was now on the defensive.

ABC News Headlines, 27 June 2012

The last word in this particular episode goes to Telstra, who made the following comment:

> "Firstly, it's crucial for me to point out that our customers' trust is the most important thing to us, so upon hearing concerns about the development of our new cyber-safety product we have stopped all collection of website addresses for its development.
>
> We've made this decision as part of our acknowledgement that more consultation was needed before launching this service."
> [http://exchange.telstra.com.au/2012/06/27/update-on-telstras-mobile-cyber-safety-tool/]

What's the problem? …

Telstra was developing a new service for their users that would allow users a more secure experience. They started the basic data collection for this new service, and users complained. Telstra said that they had stopped the program and noted customers' concerns. What's the problem?

Or, perhaps being ever so slightly cynical, Telstra was developing a new product that would allow them to charge a premium to users who were willing to opt in, and commenced a data gathering exercise that accessed public web sites. Again, what's the problem?

With a touch more cynicism one could surmise that they were attempting to address a natural concern that many parents have over the extent to which their children can access entirely inappropriate content using their mobile device and they were attempting to exploit this concern by introducing a premium product for mobile data users. But often one person's exploitation is another's useful service, and it could certainly be argued that these concerns are indeed very real and perfectly valid, and if this product meets a consumer need, and its an opt-in service, then, once more, what's the problem?

I believe that there is a problem here. And its embedded in the evolving attitudes we have related to in our respect for an individual's privacy.

More specifically, it seems to me that somehow we've managed to cross a dangerous line in the last few years about the role of a common carrier in today's digital environment.

It used to be that telephone carriers operated under the ethos, if not the entirety of a comprehensive regulatory framework, of a *common carrier*. Within the Australian framework employees of Australian public telecommunications carriers used to be required to sign a statement indicating that they were aware of the provisions of the Australian Telecommunications Act, and that divulging the contents of user's activities as they passed across the public carriage network, or indeed divulging any information relating to customer's use of the network, or tapping into customers' use of the network for reasons other than operational necessity, exposed the individual employee to criminal prosecution. The

outcomes of such prosecution allowed for hefty fines and incarceration if found guilty. The intent was simple: Customers could use the network and trust that what they said to each other was a private conversation. Neither other users of the public network, nor the carrier and its employees and agents were allowed to be privy to any conversation that occurred over the public carriage service. And, with the exception of the provisions of lawful interception, the customer's right to a certain level privacy was ensured through these provisions.

But that was then. Apparently today is different.

Here is a case not only of inspecting the user's activities without the user's knowledge and certainly without their consent, but then reaching inside the network conversation and eavesdropping upon the user's digital conversation, extracting parts of the content of this conversation and passing it offshore to a third party. This third party then apparently uses this information in ways that are way beyond the user's reasonable expectation of the limits of the role of a common carrier. It seems that such actions are way beyond the terms and conditions of the Australian Telecommunications Act, in so far as that parts of a user's conversation have been intercepted by the public carrier, recorded, and then sent to a third party without consent. All this without any form of identified operational necessity in terms of the well being and integrity of the network itself. It was a case of stalking, and that is not part of the legitimate role of a common carrier.

Why would a common carrier who enjoys a privileged position with respect to being privy to user's private conversations pay so little heed to its common carrier role?

What's so special about the role of a common carrier anyway?

What's so special about a common carrier role anyway?

There once was a time when you could not trust the messenger. There once was a time when not only did you pay to have your message sent, but you paid to receive messages. And there was no guarantee that the message would not be read by the messenger. It could be that the contents of your note could be used to determine how much the receiver should pay for the message. It could be that your message was copied and sold to other parties. If you can't trust the messenger then communications becomes a risky business.

Throughout history the position of a messenger has been a mixed blessing. To be the bearer of bad news was not an enviable role, and rather than being rewarded for the effort of delivering the message, the messenger may well be in dire straits given the level of wrath of the recipient. The option of reading the message before delivering it could be seen as a personal survival strategy, as well as being a prudent business move - bad news could be discarded immediately, while good news could attract the potential of extracting a higher delivery fee from the recipient. Of course while this may be good for the messenger, such a mode of operation was not be for the benefit of all. For the parties attempting to use the messenger service, message delivery could be a very haphazard affair. If the message itself was intended to be a secret, then one could confidently anticipate that this secrecy was going to be compromised by the messenger and that the supposedly private message would be passed on to others.

> One important way we addressed this was through the organisation of the postal system, where the postal service was operated by the public administration as a public service, and its operation was undertaken with the framework of a common carrier role. The postal carrier was not liable for the content it carried, and it treated all messages in the same manner. In return, customers of the service could use this medium in the confident expectation that in the normal course of events their envelopes would not be opened by the postal carrier. That their private conversations conducted over this service were just that - private.

These days we no longer see a position of restraint on the part of data carriers, and rather than operating in a common carrier role we are witnessing a pervasive and possessive attitude of "all your packets belong to us."

I think its encouraging to observe that there is still a body of opinion that thinks its unethical, and even plain wrong, for a carrier to stalk its customers so intensely. Moving customer data across borders to other countries may be cost effective in a business sense, but what protections accompany the data export? From an Australian perspective does a US regulatory framework protect any rights to privacy for individuals who are to them simply "aliens"?

The issues relating to the consumer's reasonable expectation of a common carriage service to be operated within basic terms of integrity and privacy are important underlying issues here. Having a common carriage provider spy of your every move via a third party operating in a different regulatory and legal regime, is not consistent with any reasonable expectation of integrity of the operation of a public carriage service. This offshore third party is in a unique position to monetize this collected information without further regard to duty of care with respect to individuals' privacy. This is not exactly a healthy development, as far as I can tell.

In more general terms it's pretty clear that in our digital environment content providers and aggregators are being seen as the beneficiaries of the promised generation of wealth. And there is no doubt that some of these more innovative content-oriented companies, such as Google, enjoy the almost euphoric confidence of investors these days. It's equally true that the previous dominant forces in this space, yesterday's telephone companies, like the newspaper businesses, are seeing the inexorable waning of their wealth, power and status as a consequence of this shift in the landscape.

For the carriers maybe there was a small beacon of hope. For a brief moment it seemed that while we had transformed the wired copper world into a revenue wasteland that offered only the promise of a future digital slum, the mobile world would be the new golden path. Mobile devices offered the combination of utility services and affordable luxury goods, and everything about this environment was growing. Demand was growing, revenue was growing and margins were extremely attractive. Maybe if they concentrated in the mobile sector they could stop this inexorable commoditization of their carriage role and transform themselves back from being a nondescript utility operator to being a valued and valuable service enabler.

But in many markets the mobile good times for the carriage providers are now also waning. As we try to expand the size of the market we have to reach into market segments that have lower discretionary levels of spending power. In addition, the high operating margins attract more competitive entrants into the market, and as a consequence both retail and wholesale carriage prices are on the way down. And in the same fashion as we've seen the operating margins for wired Internet carriage services fall over the past decade, we are now seeing this being replayed in the mobile world. But mobiles was the Plan B for the legacy telephone operators when the wired telephone became a revenue wasteland. And this time there is no Plan C for when the mobile market also becomes a commodity market, and

operating margins shrink to a level that only sustains the most efficient of operators who have the most modest of margin aspirations for their carriage role.

Perhaps it's now desperation time for these carriers. Perhaps in their search for any form of additional revenue they have taken a leaf from Google's and Facebooks's operating manuals. In the content world knowledge of the customer is *everything*.

> As Hal Varian, a noted economist in this information space observed some time back, spam is merely a failure of information about the consumer. If you knew all there was to know about that consumer then you could ensure that what you sent to the consumer was not unwanted digital detritus but timely and helpful advice!

In their desire to emulate these hypergiants of the content world I suspect that the carriers have been over-enthusiastic in their quest to know absolutely everything about their customers and what they do. In the carriage world there are few digital exhaust vents where a carrier can quietly pick over the exhaust data and pull out individual customer behaviours. But there is live traffic. Real time behaviours of real individuals working, playing and living on these carriage services. And the temptation to tap into this rich vein of data and monetize it is probably overwhelming at times. So overwhelming that in Telstra's case they appeared to simply forget about the duty of care that they have to members of the public as an intrinsic part of their responsibilities as a common public carrier.

It is often said that the road to hell is paved with the best of intentions – that the ultimate outcome of the solution is potentially far worse than the immediate problem being addressed.

It's possible to believe that this was indeed an innocent well-intentioned case of a carrier trying to offer a premium service to its users to meet a perceived market need, and at the same time differentiate itself from its competitors. After all, its often easy to confuse malice and incompetence, and ascribe to malice or evil intent a set of actions that are just as easily the outcome of simple incompetence. And incompetence is very common!

But sometimes that road to hell is one that is paved and directed by darker motives.

At times its not all about the purity of intention. Sometimes this is indeed about exploiting or even abusing a privileged position of trust for base motives of revenue opportunities. By taking a carriage role and transforming it into a cynical data gathering exercise its hard to say that the noblest of intentions was evident. There is no doubt that tapping into the digital stream reveals an extremely rich stream of information about individuals and, to put it crassly, their purchasing needs and desires.

Of course one should be wary of dichotomies, and particularly wary of false dichotomies! Maybe its a more confused story.

We have been generating mixed signals about the common carrier role for many years.

On the one hand the content folk have been extremely successful in resisting the pressure to cross-subsidise carriage providers. The various cries for "sender pays," "QoS settlements" and even "network neutrality" are all outcomes of this particular fight, and once more the policy and political level has been dragged into the fight. This time the pressure from the content giants and end user lobby groups has been to restrict the carrier as a neutral, impartial and disinterested party with respect to content being carried over the network. Carriers should indeed act in every respect within the convention of a common carrier.

But there have been other conversations and strident demands as well. When spam emerged as a significant problem the immediate reaction from many folk was to place the carriage provider into the role of anti-spam enforcer. The major complaint heard from the carrier's helpdesk and from the carrier's public affairs group was that the access provider, in effect the local carrier, was the responsible party here. The access provider should have, and enforce, "appropriate use" policies and take out these offending spammers. What was going on here was that the carrier was being cast in a role where it was perceived as being responsible for the actions of, and content generated by, their customers. And those access providers who took a principled position that this was none of their business were often shunned by their Internet Service Provider peers, and castigated by the anti-spam lobby as being "spam friendly."

It did not stop there.

> It rarely does!

When the Intellectual Property Rights folk entered the fray and complained about users trading in stolen content naturally the access carrier was seen as being the focal point for enforcement. Law Enforcement Agencies also took the expedient view that the fastest way to the end user and their activities was though their local access carrier. The IPR lobby group has been very successful in making this case of carrier responsibility at the policy and political level in many national regimes, and the LEAs saw this in a largely positive light. The result is that the carrier is being cast into a role of being an active entity in terms of both users' activities and the content being carried over the network. As a consequence the carrier is left with the impression that nobody cares about common carrier roles and it's now a free for all about mining the rich vein of the data trail generated by individual users.

Little wonder that carriers are confused about their role with respect to the common carrier provisions. Everyone else is being very busy sending mixed signals!

The ultimate outcome of continual erosion of the common carrier role is that public users of a public communications service can confidently expect all their communications to be monitored, stored and cross referenced, and later acted on by third parties in ways that are uncontrollable, unrequested and potentially unwelcome and personally damaging. Its not just that everything you post on Facebook will be with you for the entirety of your life and for a long time thereafter. Its more than that. It's everything you do, every mail you post, every purchase you make, every site you visit, everything. It's digital stalking at its most intrusive, and at its most threatening.

Maybe its time once again to phrase a coherent and consistent view of our expectations about public communications carriers and their obligations in relation to their public community of users and usage.

Perhaps it's time to resolve some of these confusing signals we've been generating. Perhaps liberalisation of the regulatory regime is not the same as discarding the common carrier role and its attendant obligations. Common carriers should have a clearly bounded set of responsibilities with respect to both content and their liability with respect to actions of clients of the service. Perhaps its time to consider how best to enforce social norms on the Internet without compromising a common respect for the basic integrity of the carrier as a neutral party to the content being carried across the network. Perhaps its time to recognise that in this domain the Internet is not novel, and what we have learned from a rich history of carriage provision in society has direct relevance to the Internet today.

The Internet is simply too valuable an environment to have its long term potential as a stable universal communications platform mindlessly sacrificed on the altar of short term business expediency and confused political signals.

Afterword: Australian Telecommunications Interception and Access Laws

Interception of telecommunications in the Commonwealth of Australia is governed by the Telecommunications (Interception and Access) Act 1979, as amended in June 2006.

To quote the Explanatory Memorandum of the 2006 Act:

> *In relation to both telecommunications interception and access to stored communications, the Act makes clear that the general position is that these activities are prohibited, except in certain clearly defined situations. This reflects the primary focus of the Act which is to protect the privacy of communications.*

The terms **communication** and **telecommunications system** are defined in the Act as follows:

> ***communication*** *includes conversation and a message, and any part of a conversation or message, whether:*
> *(a) in the form of:*
> *(i) speech, music or other sounds;*
> *(ii) data;*
> *(iii) text;*
> *(iv) visual images, whether or not animated; or*
> *(v) signals; or*
> *(b) in any other form or in any combination of forms.*
>
> ***telecommunications system*** *means:*
> *(a) a telecommunications network that is within Australia; or*
> *(b) a telecommunications network that is partly within Australia, but only to the extent that the network is within Australia; and includes equipment, a line or other facility that is connected to such a network and is within Australia.*

Section 7 of this Act states:

> *(1) A person shall not:*
> *(a) intercept;*
> *(b) authorize, suffer or permit another person to intercept; or*
> *(c) do any act or thing that will enable him or her or another person to intercept;*
> *a communication passing over a telecommunications system.*

A person who contravenes this section is guilty of an offence punishable on conviction by imprisonment for a period not exceeding 2 years. Limited exceptions to this interception prohibition are specified in other subsections of Section 7 of this Act. These include interception under an interception warrant, where such warrants may be issued for the purposes of national security and law enforcement. These exceptions also include provision for carriers and employees of carriers undertaking their duties:

> *Exceptions applicable to carriers and carrier employees in relation to duties involving the installation of lines and equipment or the operation or maintenance of a telecommunications system.*

This is further defined in the Act as:

> *An act or thing done by an employee of a carrier in the course of his or her duties for or in connection with:*
> *(i) the installation of any line, or the installation of any equipment, used or intended for use in connection with a telecommunications service; or*
> *(ii) the operation or maintenance of a telecommunications system; or*
> *(iii) the identifying or tracing of any person who has contravened, or is suspected of having contravened or being likely to contravene, a provision of Part 10.6 of the Criminal Code;*

if it is reasonably necessary for the employee to do that act or thing in order to perform those duties effectively.

This material on the Telecommunications (Interception and Access) Act has been assembled from the Electronic Frontiers Australia resource on interception and access at:
https://www.efa.org.au/Issues/Privacy/tia.html

Was it "reasonably necessary" for Telstra to direct its employees to intercept customers' communications and pass these details to a third party? Was this a reasonable part of the functions of the operation or maintenance of the mobile telecommunications system?

If this is a question about what is "reasonable" under these circumstances, then I'm of the personal opinion that this was certainly not a reasonable action in terms of the operation and maintenance of their telecommunications system. I am therefore of the opinion that this action by Telstra and its employees in undertaking interception of customers' traffic and passing details of the content of that intercepted traffic to a third party appears to constitute a breach of Section 7 of the Telecommunications (Interception and Access) Act.

Is any local regulatory agency showing an interest in pursuing this and initiating a prosecution action? Nothing to report so far.

Disclaimer

About the Author

Geoff Huston B.Sc., M.Sc., has been closely involved with the development of the Internet for many years, particularly within Australia, where he was responsible for the initial build of the Internet within the Australian academic and research sector. He is author of a number of Internet-related books, and has been active in the Internet Engineering Task Force for many years.

www.potaroo.net