CM2302 - Communication Networks and Pervasive Computing.

Smartphone Directory Investigation.

Geraint Harries, 1100682

Investigate and find information from the provided directories.

To browse through the databases I used SQLite Database browser.

To convert time/date stamps I used a UNIX time/date converter at http://www.onlineconversion.com/unix_time.htm

1. Email

File:	mailstore.pervasive@gmail.com.db
Database:	messages
Directory:	*data/data/com.google.android.gm/databases/*

Text	Sender	Receiver	Subject	Time/Date Stamp	Converted Time/ Date stamp
facebook [image] Per, you have more friends on Facebook than you think. Findi...	"Facebook" <notification+kr4yae2myxnn@facebookmail.com>	"Per Kiani" <pervasivec@gmail.com>	Per, you have more friends on Facebook than you think...	1356206584000	Sat, 22 Dec 2012 20:03:04 GMT
[image] Pervasive Computer, Here are accounts similar to who you followed. [i...	"Twitter" <n-creinfvirp=tznvy.pbz-63c71@postmaster.twitter.com>	"Pervasive Computer" <pervasivec@gmail.com>	Suggestions similar to NASA and Neil deGrasse Tyson	1356101227000	Fri, 21 Dec 2012 14:47:07 GMT
facebook Hi Per, Sorry that you've been having trouble logging into your Face...	"Facebook" <update+kr4yae2myxnn@facebookmail.com>	"Per Kiani" <pervasivec@gmail.com>	Getting back onto Facebook	1356350020000	Mon, 24 Dec 2012 11:53:40 GMT

Text	Sender	Receiver	Subject	Time/Date Stamp	Converted Time/ Date stamp
[image: Google+ team] Visit Google+ Hey Per, Welcome to Google + - we're glad ...	"Google+ team" <noreply-daa26fef@plus.google.com>	"" <pervasivec@gmail.com>	Getting started on Google+	1356355251000	Mon, 24 Dec 2012 13:20:51 GMT

2. Quick Search Box

File:	qsb-history.db
Database:	history
Directory:	*data/data/com.google.android.googlequicksearchbox/databases*

Query	Time/Date Stamp	Converted Time/Date Stamp
what is pervasive computing	1356355816533	Mon, 24 Dec 2012 13:30:16 GMT
how to be a pervasive computer	1356355862064	Mon, 24 Dec 2012 13:31:02 GMT
is star trek real	1356355901516	Mon, 24 Dec 2012 13:31:41 GMT
where is santa	1356355948654	Mon, 24 Dec 2012 13:32:28 GMT

3. Twitter

File:	1022513670.db
Database:	statuses
Directory:	*data/data/com.twitter.android/databases*

Within the database browser executed the SQL Query

```
Select *
From Statuses
Where author_id = "1022513670";
```

to select the tweets from the @pervasivecomp account. The pervasivecomp account has the author_id 1022513670.

Content	Latitude	Longitude	Retweet Account	Place Name	Sent	Place Bounding
Tweet tweets	n/a	n/a	0	n/a	Sent	n/a
Tweet	n/a	n/a	0	n/a	Sent	n/a
#winter http://t.co/drjVWqKv [Image 1 Below]	n/a	n/a	0	n/a	Sent	n/a
Rain	n/a	n/a	0	n/a	Failed to send	n/a
#Rain	n/a	n/a	0	n/a	Failed to send	n/a
#Rain http://t.co/wqcQXXyA [Image 2 Below]	n/a	n/a	0	n/a	Sent	n/a
#winterrain http://t.co/3qgp4QAK [Image 2 Below]	51.504399	-2.515792	0	South Gloucestershire	Sent	[[51.4159,-2.710705],[51.4159,-2.25212],[51.6824014,-2.25212],[51.6824014,-2.710705]]

Image 1 - #winter

Image 2 - #Rain, #winterrain

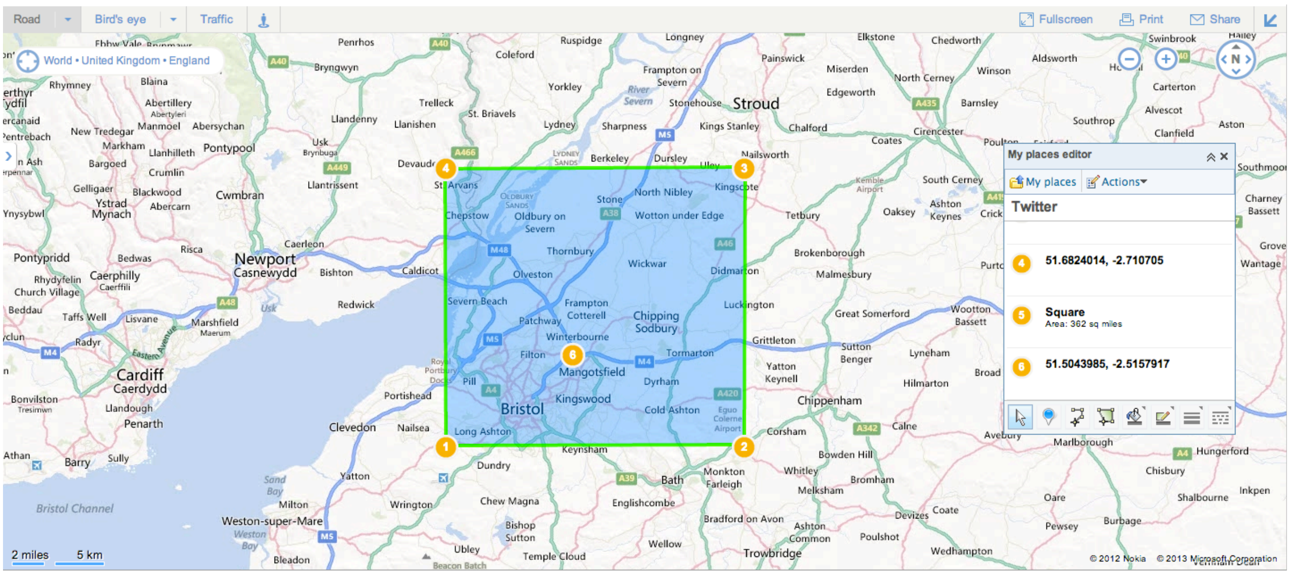
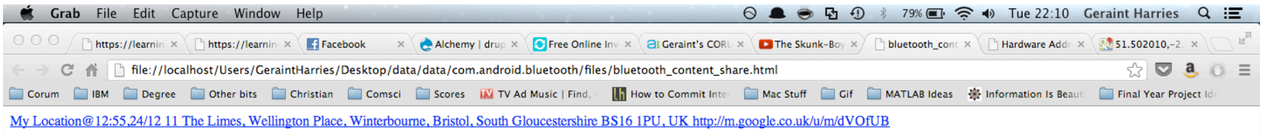


Image 4 - Mapped image with image bounding

4. Bluetooth

File:	bluetooth_content_share.html
Directory:	*data/data/com.android.bluetooth/files*

This file contained a webpage (shown below)


file:///localhost/Users/GeraintHarries/Desktop/data/data/com.android.bluetooth/files/bluetooth_content_share.html

My Location@12:55,24/12 11 The Limes, Wellington Place, Winterbourne, Bristol, South Gloucestershire BS16 1PU, UK http://m.google.co.uk/u/m/dVOfUB

Image 3 - An image of the bluetooth_content_share.html file

The text from the hyperlink is:

> *My Location@12:55,24/12 11 The Limes, Wellington Place, Winterbourne, Bristol, South Gloucestershire BS16 1PU, UK http://m.google.co.uk/u/m/dVOfUB*

Broken down this is 3 parts; the date and time, 12:55, 24/12; the location, 11 The Limes, Wellington Place, Winterbourne, Bristol, South Gloucestershire, BS16 1PU, UK, and a map URL; *http://m.google.co.uk/u/m/dVOfUB*. This means that the last time the device was seen in the vicinity of the phone was at 12:55 on the 24th of December

At the end of the hyperlink on the page is the URL "http://m.google.co.uk/u/m/dVOfUB". This is a URL to a google maps page which gave the latitude and longitude of the address at the beginning of the hyperlink on the above webpage.

File:	btopp_names.xml
Directory:	*data/data/com.android.bluetooth/files*

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<string name="E4:CE:8F:15:F9:D5">smacbook</string>
</map>
```

If you cross reference the MAC address with the list of registered Apple MAC addresses (from http://hwaddress.com/?q=Apple) you'll discover that the MAC address E4:CE:8F:15:F9:D5 is that it is an apple product. This confirms suspicions, given the hostname is "smacbook".

5. Google+

File:	es0.db
Directory:	data/data/com.google.android.apps.plus

Last Sync Time:	Wed, 26 Dec 2012 10:13:32 GMT
Last Stats Sync:	Mon, 24 Dec 2012 16:36:26 GMT
Last Contacted Time:	Wed, 19 Dec 2012 17:51:12 GMT
Circle Sync Time:	Wed, 26 Dec 2012 10:13:09 GMT
People Sync Time:	Wed, 26 Dec 2012 10:13:09 GMT
Suggested People Sync Time:	Mon, 24 Dec 2012 16:36:05 GMT
Event Themes Sync Time:	Tue, 25 Dec 2012 21:08:44 GMT
Last Analytics Sync Time:	Wed, 26 Dec 2012 11:52:40 GMT
Last Settings Sync:	Tue, 25 Dec 2012 21:08:19 GMT
Last Emotishare Sync Time:	Wed, 26 Dec 2012 10:13:09 GMT

In the photo_home_cover database is a URL which corresponds to an image (https://lh5.googleusercontent.com/-q-xizKVL4po/UNiHTJTopGI/AAAAAAAAAA4/PefcLYI-LmI/s0-d/IMG_20121224_130151.jpg)

I uploaded the photo to http://regex.info/exif.cgi to get as much exif data out of it as possible. Below is the data.

Camera:	HTC Wildfire
Lens:	3.5mm
Exposure:	ISO 74
Date:	December, 24, 2012, 1:01:48PM
File:	1712 x 2560 JPEG (4.4 megapixels), 0.9 megabytes, image compression 93%
Encoding Process:	Baseline DCT, Huffman Coding
EXIF Byte Order:	Big-Endian

File:	iu.upload.db
Directory:	data/data/com.google.android.apps.plus

You can find the exact time the photo was uploaded: Mon, 24 Dec 2012 13:01:48 GMT. This is exactly the same time the photo was taken (see above) so the HTC must have used Google+'s instant upload. (See http://www.geeksugar.com/Google-Pros-Cons-18161469 for confirmation)

Within the locations database of the es0.db file, is list of the names of the geo-locations that the phone has shared on google+. Below is a map which shows these locations mapped within the image bounding found from the twitter image.

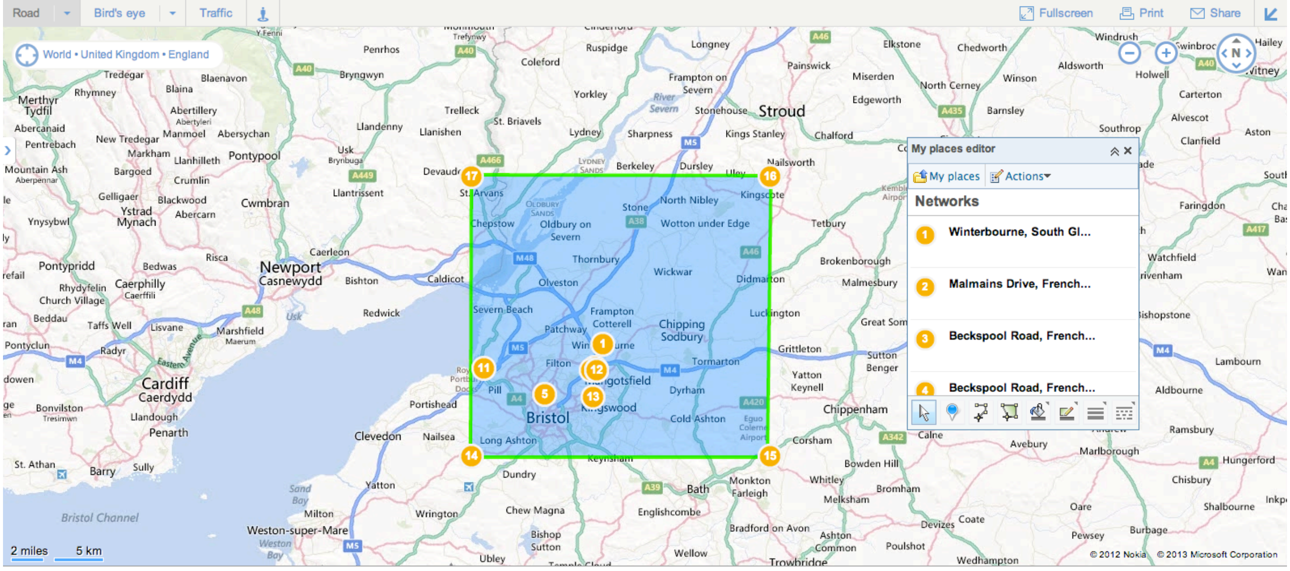

Road
Bird's eye
Traffic
Fullscreen
Print
Share
World • United Kingdom • England
My places editor
My places
Actions
Networks
1 Winterbourne, South Gl...
2 Malmains Drive, French...
3 Beckspool Road, French...
4 Beckspool Road, French...
Bristol
Cardiff
Newport
Stroud
Bath
Chippenham
2 miles
5 km
© 2012 Nokia
© 2013 Microsoft Corporation

Image 5 - Mapped Google+ locations plus the image bounding from the twitter picture

Within the contacts database of the es0.db file, you are able to all the contacts (names, ids) of the account. Most of them are celebrity accounts some are real. E.g. Per Heinz, (101002072995463170786) is obviously your account, but you can also see Saad Liaquat Kiani, (115155032534485192781).

6. Wi-fi

File:	wpa_supplicant.conf
Directory:	data/misc/wifi/

```
ctrl_interface=eth0
update_config=1

network={
        ssid="slk"
        psk="sun1shine"
        key_mgmt=WPA-PSK
        priority=1
}
```

The SSID to the network slk and the password is sun1shine. [Incidentally, the gmail, twitter, hotmail and facebook accounts all have the same password. Poor security practice!]

7. WhatsApp

You can access your Whatapp avatar from /data/data/com.whatsapp/files/avatars (Shown Below)

Image 6 - WhatsApp Avatar

File:	wa.db
Database:	wa_contacts
Directory:	data/data/com.whatsapp/databases

jid	status	number	Display Name
441173283085@s.whatsapp.net		+441173283085	slkiani
447912352230@s.whatsapp.net	Hey there! I am using WhatsApp.	07912352230	Saad Liaquat
441179028264@s.whatsapp.net		+441179028264	slkiani
447912352230@s.whatsapp.net	Hey there! I am using WhatsApp.	+447912352230	slkiani

File:	msgstore.db
Database:	messages
Directory:	data/data/com.whatsapp/databases

Data	Time/Date Stamp	Received Time/Date Stamp	Receipt Server Time/Date Stamp
Hi Saad.	Mon, 24 Dec 2012 13:25:08 GMT	Mon, 24 Dec 2012 13:25:08 GMT	Mon, 24 Dec 2012 13:25:09 GMT

8. Skype

File:	config.xml
Directory:	data/data/com.skype.raider/files/live#3apervasivec/

Skype Last used: Mon, 24 Dec 2012 13:10:56 GMT.

File:	eas.db
Database:	properties
Directory:	data/data/com.skype.raider/files/live#3apervasivec/

Name:	Saad Liaquat Kiani
Home City:	Bristol

Home State:	South Gloucestershire
Home Phone:	+441179028264
Mobile Phone:	+447912352230
Email:	pervasivec@live.com

File:	eas.db
Database:	contacts
Directory:	data/data/com.skype.raider/files/live#3apervasivec/

Skype Name	Full Name	Address	Phone Numbers	Profile Time/Date Stamp	Last Online Time/Date Stamp	Last Used Time/Date Stamp
echo123	Echo / Sound Test Service			Tue, 15 Mar 2011 09:21:00 GMT		
slkiani		Bristol, South Gloucestershire, gb	home: +441179028264 office: +441173283085 mobile: +44 7912352230	Sat, 01 Jan 2011 16:20:02 GMT	Mon, 24 Dec 2012 13:50:54 GMT	Mon, 24 Dec 2012 13:11:19 GMT
live:pervasivec	Pervasive C			Mon, 24 Dec 2012 13:06:59 GMT		

If you look at the calls database in main.db you can confirm that the last used time/date stamp is correct as the only call made from slkiani was Mon, 24 Dec 2012 13:08:35 GMT

File:	eas.db
Database:	messages
Directory:	data/data/com.skype.raider/files/live#3apervasivec/

To	From	Time	Message
slkiani	Pervasive C	Mon, 24 Dec 2012 13:08:04 GMT	Hi, I&apos;d like to add you as a contact on Skype. Pervasive C
Pervasive C	slkiani	Mon, 24 Dec 2012 13:08:31 GMT	

To	From	Time	Message
slkiani	Pervasive C	Mon, 24 Dec 2012 13:08:42 GMT	<partlist alt=""> <part identity="live:pervasivec"> <name>Pervasive C</name> </part> <part identity="slkiani"> <name>slkiani</name> </part> </partlist>
Pervasive C	slkiani	Mon, 24 Dec 2012 13:09:47 GMT	Hi Pervasive C, how are you doing?
slkiani	Pervasive C	Mon, 24 Dec 2012 13:11:19 GMT	Ok.

9. Google Talk

File:	talk.db
Database:	messages
Directory:	*data/data/com.google.android.gsf/databases*

Body	Time	Type
Hi	Mon, 24 Dec 2012 16:35:00 GMT	0
hi bsck	Mon, 24 Dec 2012 16:35:19 GMT	1
Whats up??	Mon, 24 Dec 2012 16:35:51 GMT	1
hi bsck Whats up??	Mon, 24 Dec 2012 16:35:51 GMT	1
Nothing	Mon, 24 Dec 2012 16:36:10 GMT	0
good	Mon, 24 Dec 2012 16:36:15 GMT	1
What?	Mon, 24 Dec 2012 16:36:25 GMT	0

Body	Time	Type
Nothing	Mon, 24 Dec 2012 16:36:32 GMT	1
Ok	Mon, 24 Dec 2012 16:36:39 GMT	0

10. Configured Accounts

File:	accounts.db
Database:	accounts
Directory:	*d*ata/system/

Name	Type	Password
pervasivec@gmail.com	com.google	AFcb4KQB7zueeMAOG0w30l5QaEx_ypgEKsDfNjt_RB0YNnG3DScmAiniL2OmOAiQ28_qTDO6UtbaqYqllhKjxxtqgnPi3CFq9e1wYD84laJpvLZKMze7xyOmf3RIj0MgdoPmXvPTT9lmMqlA2z0NY8-rKaguPI8Q6mI91JlcxqAFVrbkHg==
live:pervasivec	com.skype.contacts.sync	639495
pervasivec@live.com	com.android.exchange	sun1shine

What is the significance of this information becoming known if you lose your phone?

I believe that this information is very significant. For example, from this phone data I've been able to access:

- Gmail Username, Password and recent Emails
- Recent Searches
- Twitter Username, Password and recent Tweets (including images with geo-location data)
- Address
- Computer Name and Model
- Google_ stats and photos
- Phone Camera Spec
- Google+ Locations
- Wifi Username and Password
- WhatsApp messages
- Home and Mobile phone number
- Skype Contacts and conversations
- Google Talk Messages

Using a combination of this information, I could, log on to your home wifi, log in to your twitter, facebook, skype (by using the @live account to reset the password) and gmail accounts, phone your home number. As I know your address, I could phone your home number to see if you are in and if not break in.

This is quite a typical phone, it has several social media sites and email accounts associated with it and accessible through it. This is a very similar set up to my smartphone. Although my phone is a different make, I'm sure once the system and user files are accessed it is as easy to interpret them as with this phone.

I have stored in my phone, a list of several contacts and their corresponding emails, very personal and important emails as well as wifi keys and locations of regular wifi networks I use. This task has been a frightening alert to how much key information is stored in our smartphones and how slack the security is compared to our personal computers. I encrypt my laptop and back it up regularly and yet have never considered either with my phone, even though it accesses the same information.

This information is very significant and if stolen and maliciously used, would cause an unrecoverable security breach. For example, if someone knows a password, they can reset a password. This means they can totally take over an account and the legitimate user is helpless to stop them.

Consequently the significance of this information becoming known if I lose my phone is incredibly high. Not only can someone access my data, they can actively remove my connection to it and use accounts in the guise as me. My main worry if my phone was stolen and used maliciously, is I have applied for internships and have several emails in my inbox from companies with offers and jobs, one of which I have accepted. If an attacker really wanted to do damage, they could email the company and ask to withdraw from the scheme.

For any one category of information discovered, describe how you could re-design the software such that the stored information remains inaccessible through an exercise you have performed in step 1.

Given increasing network and internet speeds and the increase in cloud storage, one way to eliminate sensitive data being stolen when a phone is stolen, is to de-localize the information to the cloud. That way if the phone is stolen, if the “Hacker” doesn’t know the password and key, they are unable to access the information from the cloud. The key could be stored encrypted in the phones system files.

However, with the cloud storage, you would have to make sure that the data was secured correctly. As if you don’t you would have the same problem if someone was able to bi-pass the security and get at the data. You could do this by encryption of data and having heightened security firewalls. With high security in place, there should be less of a security risk than left locally.

Rather than using passwords, you could use information that was totally unique to the user (Biometric information). For phones, obviously fingerprint scanners would be too bulky to add on, however something like face recognition would be very useful. Several phones at the moment adopt this method.

If were to apply these software changes to one category, it would be the google+ location data. From the google+ locations, the users house and regular places were found. This could be very dangerous if the “hacker” and a particular grudge against the user and wanted to harm them or their family. Therefore this data would be best put securely in the cloud and not locally on the device. Hence why

You may be an advanced user of modern technology; you can probably put in place measures to safeguard your on-device information. What about the average user, should this category of users be concerned if they were to become aware of information in categories 1.i to 1.xix being so easily retrievable?

i. What actions can they take to safeguard their information?

Users can use encryption to safeguard their information, for example, on an android device there are only a few steps to totally encrypt your phone. None of these steps are particularly hard so much so that any android user could easily complete them.

Go to *Settings* > *Personal* > *Security* > *Encryption* > *Encrypt Phone* > *Encrypt.* After that, all you have to do is enter your PIN and touch *Encrypt Phone*. The encryption process starts and once finished will ask for your PIN again. This process is as simple (if not simpler) for many of the popular smartphone models.

In addition to native smartphone encryption, there are also several apps available to encrypt your data further.

Encryption is all well and good if you know about it, but if you don't you may only consider getting it too late. This is why educating the user is very important. If the user understands how much sensitive data is held on their phone and also how they can protect it, security and privacy problems would largely reduce.

If, as part of the setup of the phone, the importance of encryption was explained and users were advised to enable it, users would not only understand the problem but would have implemented a solution. Similarly the same applies for applications that are designed to remote wipe the phones information. If users were more aware of these services then they would be much more inclined to use them.

Do you expect a significant change in how you utilize your smart phone?

I found it alarming how much information was easily accessible from just using a database browser on the phone data. I have certainly thought about my the personal security on my phone.

I have decided to enable a much more secure password. I have an iPhone so setting that up is very easy *Settings* > *General* > *Passcode Lock* > *Simple Passcode* > *Off.* Rather than being a 4 digit code, this enables your password to include letters and symbols. Although I didn't need to crack a password for this coursework, when initially getting the data a password must have been got around. By using a more secure password, this makes it more difficult for someone to get the system and user files and consequently can't interpret data from it.

I also have deleted linked email accounts from my phone. I learnt from this task that if you access to an email account you potentially have access to everything. You are able to reset passwords using usernames and emails and consequently can get into any account if you have access to the email accounts.

I have also decided to encrypt my iPhone as iPhone's are very easy to encrypt. Very little of the data was encrypted on the android device, by encrypting it you are adding another layer of security. The "hacker" needs to have your passcode to be able to decrypt the information.

This has been a very enlightening experience for me as a smartphone user. I am glad that I was able to learn about it this way than through a security breach experience.

Will privacy and security concerns like the ones discovered in this exercise limit the adoption of pervasive technologies and services in the long run? Or will an unaware public blindly follow these advancements with little conscious regard to their privacy and security? What trends do you foresee?

With the increase into security and cyber-terror, I think it will be long before the public are more aware of privacy and security matters.

MI5 Head, Jonathan Edwards said in a speech in 2010, "The overall likelihood of any particular entity being the subject of state espionage has probably never been higher, though paradoxically many of the vulnerabilities exploited both in cyber espionage and traditional espionage are relatively straightforward to plug if you are aware of them"

With increased media coverage of security and privacy issues (such as activist group anonymous, regular Facebook privacy issues and company), the public are becoming ever more aware of security risks and privacy matters and yet don't implement any solutions to combat against these risks. If you take the Sony 77 million user data loss from 2011, users are fully aware that their data can be breached and seem to add no extra security measures.

Alongside this, users persistence in adopting the cloud with very little understanding of it or the security consequences. This proves that consumers blindly follow the trends rather than stepping back and thinking of the security and privacy ramifications. For example, dropbox has over 100 million users, however I doubt many of them read the terms of server or even know where their data is being kept. The terms of service are read so rarely that there is a market for sites like http://tosdr.org, which explicitly state good and bad areas of the terms of service for companies.

For their to be a public paradigm shift regarding security, a very significant would have to happen to the general public. It would have affect a ubiquitous service such as Facebook or Twitter for people to change their outlook on security.

I predict in the near future a lot of "small time" security breaches that the public will either ignore or tolerate. However, in the distant future, I predict one large scale security breach of a ubiquitous service which will alert users to the reality of security.

Bibliography

“Jonathan Evans' terrorism speech.” Available: http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8008252/Jonathan-Evans-terrorism-speech.html. Last accessed 8th March 2013.

“PlayStation Network hackers access data of 77 million users.” Available: http://www.guardian.co.uk/technology/2011/apr/26/playstation-network-hackers-data. Last accessed 8th March 2013.

“Dropbox hits 100 million users, looking for great Dropbox stories.” Available: http://www.tuaw.com/2012/11/14/dropbox-hits-100-million-users-looking-for-great-dropbox-storie/. Last accessed 8th March 2013.

“How to encrypt an iPhone”. Available: http://www.ehow.com/how_6923548_encrypt-iphone.html/. Last accessed 8th March 2013.

“iOS Encryption is so good, not even NSA can hack it”. Available: http://gizmodo.com/5934234/ios-encryption-is-so-good-not-even-the-nsa-can-hack-it. Last accessed 8th March 2013.

“Encrypt your phone”. Available: http://support.google.com/android/bin/answer.py?hl=en&answer=1663755. Last accessed 8th March 2013.

“Avira, Free Android Security”. Available: https://play.google.com/store/apps/details?id=com.avira.android&hl=en. Last accessed 8th March 2013.