Mobile Devices have made us the most monitored individuals in history

SEM2220 - Assignment 4

090932464

Contents

1 Introduction

There has been a lot of news in the press in the last year about surveillance programs run by many countries security agencies, particularly focused on the collection of phone records by the National Security Agency (NSA)[1].

It comes as no surprise that this has brought about the question:

"Have mobile devices made us the most monitored individuals in history?"

To fully understand the depth of this question, one must consider the technical methods which are employed to monitor mobile devices and how these methods differ across different mobile platforms. In hand with this, one must investigate the methods for preventing unwanted monitoring on mobile devices and how effective these methods really are.

Finally there are many legal and professional issues which govern the collection of data from mobile devices; but there are also a host of ethical and social issues which legal and professional element cannot, necessarily, cover.

Of course monitoring of data, especially from mobile devices, doesn't have to be used for nefarious purposes. Applications commonly use data mining techniques to provide a better experience for their users and cloud services are so popular that imagining a world where all a users data is stored solely on a single device is almost impossible.

2 Technical Methods for Monitoring Mobile Devices

Because of the structure of the Global System for Mobile Communications (GSM), any mobile device which accesses the mobile network can be tracked to, at worst, the nearest cell tower. In fact the NSA is known to use this data to track targets and identify possible accomplices[2]. There are also other stories of UK public organisations performing similar actions[3][4].

Though this is a worrying concept, there is some important information that the U.S. has given in [5] which denies that any information collected cannot be used to target any individual without a prior specific and documented reason to do so. In the case of monitoring of non-U.S. citizens there must also be a agreement with the country of their citizenship.

It is the monitoring which the users agrees to have performed upon them that is perhaps more worrying.

Modern mobile platforms typically have some sort of security system and ways in which applications can be given access to secure elements of the mobile device. Most of these platforms sandbox third-party application allowing the kernel to control the access to the various facilities of the device.

2.1 Android Security Facilities

[6] describes the methods the Android system uses to secure the environment. The main advantage Android gains in this area is that runs a version of Security-Enhanced Linux (SELinux)

3 Protection Against Unwanted Monitoring

4 Implications of Mobile-based Monitoring

References

[1] G. Greenwald, E. MacAskill, and S. Ackerman, “NSA collecting phone records of millions of Verizon customers daily,” *The Guardian*, 6 Jun. 2013, [Accessed Jan. 15, 2014]. [Online]. Available: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[2] *Summary of DNR and DNI Co-Travel Analytics*, white paper, NSA, 1 Oct. 2012.

[3] R. Gallagher and R. Syal, “Met police using surveillance system to monitor mobile phones,” *The Guardian*, 30 Oct. 2011, [Accessed Jan. 15, 2014]. [Online]. Available: http://www.theguardian.com/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance

[4] N. Hopkins, “UK gathering secret intelligence via covert NSA operation,” *The Guardian*, 7 Jun. 2013, [Accessed Jan. 15, 2014]. [Online]. Available: http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism

[5] J. R. Clapper, U.S. Director of National Intelligence, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillence Act*, fact sheet, U.S. Govt., 8 Jun. 2013.

[6] *Android Security Overview*, The Android Open Source Project, [Accessed Jan. 15, 2014]. [Online]. Available: http://source.android.com/devices/tech/security/