

London calling: phone biometrics should be handled with care

December 1 2014, by Nancy Owano



Credit: Peter Griffin/Public Domain

Current and future uses of biometric data and technologies have been under review in the UK, with the British Parliament hearing views from security experts. Biometric technology identifies individuals automatically by using biological characteristics; digital consumers have been told that biometrics will be an effective alternative path for security measures against password theft and forced access to sensitive

information. Whether it's a student's bank account information or a mobile device loaded with confidential enterprise data, the toll of identity theft has sent researchers on campuses and in technology companies looking for safe authentication methods. How reliable is biometrics as applied to mobile devices? How well are vendors implementing this technology? In the UK, a Science and Technology Committee in August announced an inquiry into the use and [collection](#) of biometric data back in August. The inquiry focus was on "the potential use and collection of biometric data and whether regulations in this emerging field are adequate."

Just recently, remarks from Sir John Adye, chairman of Identity Assurance Systems, drew attention, when he express his concerns over fingerprint recognition in mobile devices to check identity. I don't know what happens to my [personal data](#) when I use it on a smartphone," he was reported by the BBC on Thursday. as telling MPs.

"I don't know, although I'm quite experienced in this area, what happens to my personal data when I use it on a smartphone for [proving](#) my identity. Is Google going to use that data to target advertising at me? Is some other commercial company or maybe some hostile foreign government going to use it to target me in some other way? I don't know," he said.

Sir John Adye's comments were made in evidence to the Commons Science and Technology Committee, in examining the use of biometric technology. Adye's comments were especially notable, as a former head of the government's GCHQ between 1989 and 1996. He now chairs a company, Identity Assurance Systems, developing [biometric technology](#) for identity recognition. "If you go to an ATM and put in your credit or debit card, that system is supervised by the bank in some way," he said in evidence to the Commons Science and Technology Committee. "But when you're using your smartphone... there's no physical supervision of

the system."

He was also quoted by the BBC as saying, "You can now use your iPhone 6 to make payments using biometrics on the internet and you've got to tick various boxes before you do so, but how many people are actually going [sic] read through all those boxes properly and understand what they mean when it goes in?"

He added, "You need to design security methods... which are going to be strong to protect the interests of the individual who is using the phone and the relying party at the other end... the bank or whoever it is, who is providing a service to them."

Matt Hanson in TechRadar reported on Friday that Apple contacted them regarding the concerns expressed by Adye over biometrics and TouchID. "On its Privacy website it states that 'the actual [image](#) of your fingerprint is not stored anywhere, and is instead converted to a mathematical representation of a fingerprint that cannot be reverse engineered into one. This mathematical representation is stored in a Secure Enclave within your phone's chip, and is never accessed by iOS or other apps, never stored on Apple servers, and never backed up to iCloud or anywhere else'."

Meanwhile, the UK Parliament website reported on Friday that "social media users may not be fully [aware](#) of how their data can be used by websites and apps given the excessive length and complexity of the terms and conditions that companies make users agree to, the Science and Technology Committee has warned." A report from the House of Commons Science and Technology Committee stated, "We are not convinced that users of online services (such as social media platforms) are able to provide informed consent based simply on the provision of terms and [conditions](#) documents. We doubt that most people who agree to terms and conditions understand the access rights of third parties to

their personal data. The terms and conditions currently favoured by many organisations are lengthy and filled with jargon. The opaque, literary style of such contracts renders them unsuitable for conveying an organisation's intent for processing personal data to users. These documents are drafted for use in American court rooms, and no reasonable person can be expected to understand a document designed for such a niche use."

© 2014 Tech Xplore

Citation: London calling: phone biometrics should be handled with care (2014, December 1) retrieved 27 April 2024 from <https://techxplore.com/news/2014-12-london-biometrics.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.