IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A flexible 802.11 element to carry privacy information | | | | |
| Date: 2014-11-12 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Mark RISON | Samsung Cambridge Solution Centre | SJH, CB4 0DS, U.K. | +44 1223 434600 | at samsung (a global commercial entity) I'm the letter emme then dot rison |

Abstract

This document proposes dedicating an 802.11 element to privacy signalling, and defining this in a flexible way which will allow it to cover privacy issues as they arise.

**Introduction**

As new ways in which privacy has been compromised through the use of wireless technology are revealed, people are getting more concerned about protecting their privacy when using wireless technology. A few proprietary ad hoc mechanisms have been introduced to try to address a few of the privacy concerns (e.g. [Google’s “\_nomap” feature](https://support.google.com/maps/answer/1725632), [Apple’s MAC address randomisation feature](http://www.apple.com/privacy/privacy-built-in/)) but these do not address the problem in a generic and flexible way (e.g. issues with fingerprinting). The only real safe solution so far is “turn off the wireless technology, then!”, but this is not acceptable to most people.

This document proposes dedicating an 802.11 element to privacy signalling, and defining this in a flexible way which will allow it to cover privacy issues as they arise.

**Basic principles of operation**

The starting point is the notion that people should have their right to privacy respected unless they explicitly waive it (this is the opposite polarity to [the HTTP Do Not Track header](http://en.wikipedia.org/wiki/Do_Not_Track)).

The 802.11 privacy element would therefore indicate which rights are being waived. Only where the rights have been explicitly waived in this way may someone’s privacy be infringed upon. In some jurisdictions such a rule may have legal backing; in others it would be an honour system (and people would be entitled to take a dim view of failure to honour it, e.g. by a boycott, public complaint or campaign to legislate).

The fields in the element could cover various privacy issues, including but not limited to:

* “you may track my location”
* “you may send me marketing/promotional/advertising material”
* “you may track my (MAC or IP) address”
* “you may log the domain names/IP addresses I access”
* “you may track me if the tracking is not associated with any identifier” (e.g. Google Maps traffic tracking)
* “you may fingerprint me (by e.g. the SSIDs I scan for)”

By the principles enunciated above, if there is another privacy issue it is covered in the negative by default, i.e. “you may not infringe upon my privacy in that way”. When such a privacy issue is identified, a new field in the element can be added (by TGm), and people can choose whether to waive their right to privacy as far as that issue is concerned.

**Possible refinements**

The fields in the 802.11 privacy element could have geographical or jurisdictional restrictions, e.g. “do not track if outside the EU”, “do not fingerprint unless the information will be processed subject to the constraints imposed by EU data privacy regulations (even if outside the EU)”, since the legal protection afforded in various jurisdictions differs.

The fields in the element could have temporal restrictions, e.g. “but delete all information collected within 24 hours”.

The fields in the element could have specific exemptions, e.g. “the operator of the network used for the London marathon (identified e.g. by SSID or HESSID) may, however, track my location”. Or restrictions, e.g. “the operator of a network in a shopping centre may not, however, track my location”.

As a further extension, there could be a mechanism to seek consent to override the privacy signalling, e.g. sending an Action frame requesting that certain fields in the element be disregarded by the sender of the Action frame, which could pop up a dialogue box asking for the user to accept or reject (or be pre-configured to auto-reject), probably in exchange for some kind of incentive, sending the reply in another Action frame.

**References**

Given above.