Comms Data and Content: can we actually separate them? a short briefing note

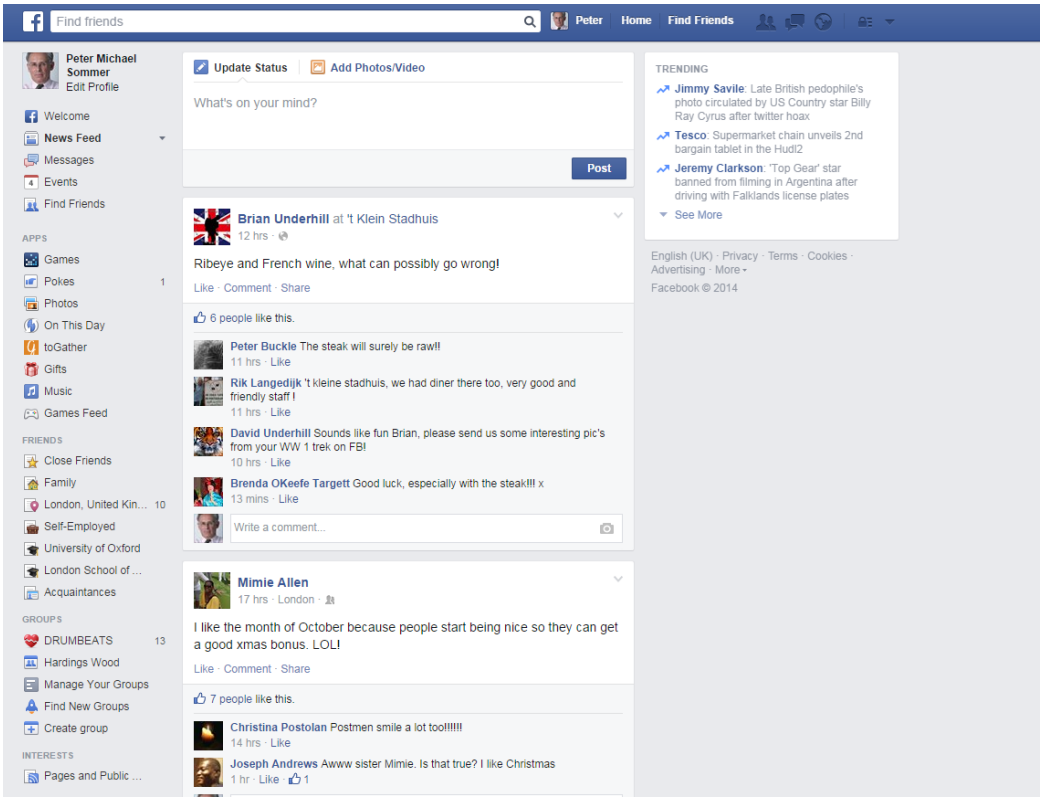
Peter Sommer

1. The structure of RIPA makes a distinction between "content" and "communications data", the former addressed in Chapter 1 of the Act, authorised by the Secretary of State and not admissible in proceedings and the latter authorised by a Designated Officer in a law enforcement agency and fully admissible. Data Retention applies only to communications data.

2. In 1985 with IoCA and to a lesser extent in 2000 with RIPA the legal definitions could readily be applied to the main communications technologies. "Comms data" was the detailed phone bill and associated subscriber information, "content" or "intercept" is what was heard across the line.

3. But on the internet and elsewhere everything is now digital data. Some types of data carry "flags" or technical markers which specialist equipment can easily look for. This applies to conventional email where the "flags" are in the "headers" generated as the email moves from author to recipient and where the email technical protocol defines each element. It also applies to identifying the start of a web-page.

4. But these markers do not exist for important types or communication. A Facebook page presents itself as a web-page but within each page are elements which are both "comms data" and "content". As a manual exercise and armed with the legal definitions a patient person can probably separate the two. This can be easily seen by examining this screenshot from Facebook.



5. The CSP, however is not going to examine each different page and carry out a manual exercise. They need an automated system – which could only exist if there were a constantly-updated set of filters to cover each type of web-page that might have a mixture of comms data and content. And even for individual suppliers, web-page designs are constantly being changed.

6. The problem will become more acute with the introductions of services such as IMS (IP Multimedia System) which allows voice, text and other multimedia services to traverse all connected networks and is of particular value to mobile internet providers.

7. Law enforcement and the agencies run a significant risk of receiving material *ultra vires* of the authorising warrants and of introducing inadmissible intercept, which will then be challenged in the courts.

8. There are important consequences:

    a. Revised Comms Data or revised RIPA legislation would need to recognise that if comms data and content cannot be separated new sets of authorising powers need to be identified, probably based on degree of intrusion

    b. The almost-unique UK rendering of content inadmissible would have to be abandoned.

6 October 2014