

Data Sharing Review

Richard Thomas and Dr Mark Walport

Consultation paper on the use and sharing of personal information in the public and private sector

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to contact@datasharingreview.gsi.gov.uk

Alternatively you can send a hard copy response to:

Data Sharing Review Secretariat
5.26 Steel House
11 Tothill Street
London
SW1H 9LJ

Thank you.

Section 1: Background

Question 1.

Comments: The Telecommunications UK Fraud Forum (TUFF) is a body who draws its membership from the telecommunication industry and its aim is to reduce the levels of fraud and crime specifically targeted towards member companies. To do this it shares information in a number of ways.

1. It gathers and shares contact details of member companies including personal details of main points of contact for enquiries in relation to fraud and crime. It also processes information detailed below in accordance with DPA Sec 29 procedures and on very rare occasions Sec 35.
2. It facilitates the sharing of specific information in relation to fraud and crime committed or attempted against member companies. Such information may include personal details such as names, addresses, modus operandi and telephone numbers associated with the case.
3. It maintains a database of those individuals who member companies have dismissed for gross mis-conduct amounting to theft or fraud. It also includes individuals who leave employment prior to or during such investigations. This information is available to be checked against individuals applying for positions within other member companies and employment contracts inform employees that such information will be exchanged within the membership.
4. TUFF also act as a point of contact for law enforcement agencies who may

be seeking information on individuals, companies or telecom related issues. Under these circumstances the requesting information is noted and then forwarded to the appropriate member(s) for their input. Where matters of sensitivity dictate TUFF may act as the "cut out" and handle the information request and replies.

5. All information is exchanged via email and where appropriate password protected. All databases operated by TUFF are themselves password protected and in the case of sensitive information this may be also additionally password protected down to file/document level.

6. The information is held on a central password protected server located within a protected area with a Redcare 24/7 security protection. Access to the server is via a closed local area network with each terminal being afforded the same levels of protection as the central server.

7. Access to the local area network from outside the protected area is achieved via the internet and requires 2 levels of security log on to access records. The server and terminals operate behind firewalls and maintain 24/7 virus protection which is updated in real time.

8. Access passwords are a combination of letters, figures, upper and lower case and are changed every 90 days or when an employee leaves

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2.

Comments: It is the view of TUFF that in order to minimise the impact of criminal activity aimed at telecommunication companies and their customers it is essential that relevant information is exchanged between telecommunication companies. Such activity often protects individual customers from becoming victims of fraud and crime. For example a telco who observes illegal activity such as hacking is able to forward this information on so that other telcos can take preventive action and protect their customers. A telco may observe unusual levels of traffic originating or terminating on customer premises equipment and this may on investigation prove to be illegal. Passing on such information is critical if the damage done by such fraud and crime is to be negated. Such information also allows other operators to condition their network surveillance equipments to detect any further abuse which in some cases prevent such fraud and crime from occurring. In terms of benefit to society such action on the part of telecommunication companies help provide a more secure environment in which society can operate reducing exposure of both individuals and collectives to this kind of activity.

Question 3.

Comments: The risks to an individual in the sharing of their personal information is that the information is in someway incorrect or not complete and as such will expose the individual to reputational or financial risk. For example an individual applying for a position on having their personal details checked against an "offenders" database must have the confidence that any such check is carried out fairly and that the process is transparent and contains the necessary checks and

balances to ensure fair and appropriate processing of the data. If such a regime is not present then there is a real danger of adverse exposure for both individuals and for society. However, a balance has to be reached to ensure that criminals or those persons intent on manipulation of personal data are not allowed to defeat the processes that are in place for the protection of individuals and society.

Question 4.

Comments: It is the belief of TUFF that the sharing of personal information within the telecommunication environment for the purposes listed under Sec 29 of the DPA provides the industry with effective crime fighting tools to enable them to investigate telecommunications crime and fraud which otherwise would go undetected. such practice also acts as a deterrent to fraudsters and criminals knowing that such information can and will be exchanged. The risks of such activity is if there is no clear procedures or processes to enable audit to take place on what information had been exchanged and under what circumstances. Such audits form part of best practice but are not legally enforceable and abuse only comes to light as a result of whistle blowing or some other such activity

Question 5.

Comments: No Input

Question 6.

Comments: No Input

Question 7.

Comments: The levels of cross industry/cross sector sharing of information is low and a higher level of engagement would be beneficial in the fight against fraud and crime. Individual and organised criminals often target different sectors at the same time or consecutively. A greater level of information sharing would enable such activity to be detected earlier and would enable different sectors to be better prepared to detect and deal with such criminality. For example greater sharing of claims information, between insurance industry and telecommunications, would enable fraudulent insurance claims for handset loss be detected and thus the loss to both industries to be reduced. It is also considered that law enforcement agencies hold information on individuals which would be of great benefit in the investigation and detection of further criminal activity. There is a reluctance on the part of law enforcement to release such information or to even confirm that such information exists

Question 8.

Comments: No Input

Section 3: The legal framework

Question 9.

Comments: It is the opinion of TUFF that in general the DPA works well. However, its weakness is in the lack of penalties that can be applied for abuse or misuse of personal data. The Information Commissioner should and must be given powers to enable him to raise fines against persistent offenders who fail to

heed warnings issued by the ICO. In the extreme cases this power should be backed up by custodial sentences.

Question 10.

Comments: It is the opinion of TUFF that the second principle is not clearly understood by all those concerned in data collection. All too often data collected for one purpose is used for another. For example data collected for customer registration has been known to be used in a marketing scenario. The spirit and thrust of the second principle is we believe sound however its execution in practice needs to be more closely regulated and audited. The ICO, or agents acting on their behalf, should proactively test the processes behind the second principle and aciton those breches that are discovered

Question 11.

Comments: institutionally there is and always has been a reluctance on the part of data holders both authorities and private business to share data. This often prevents the timely exchange of data relating to criminal activity being shared. All too often the responses to legitimate requests for data exchange are met with a negative or refusal to provide. There needs to be more clear scenarios under which personal data can be exchanged and these need to be understood by all concerned. There should also be some form of redress that can be taken in such cirucmstances by the requesting body.

Question 12.

Comments: There is a need to increase sanctions to include fines and if appropriate greater punishments for the continued abuse of personal data

Question 13.

Comments: When correctly applied Section 29 of the DPA impacts positively on the investagation of criminal activity. When its provisions are ignored or not recognised this has not only a negative impact on investigation of criminal activity but enables fraudsters and criminals to operate.

Question 14.

Comments:

Question 15.

Comments: Siubject access can place an undue burden on small to medium companies who do not have resources to deal with high volumes of requests.

Section 4: Consent and transparency

Question 16.

Comments: TUFF do not see any issues with the aspectr of personal consent to share data

Question 17.

Comments: To have to obtain consent on a cse by case basis would place an undue burden on business as well a s increase significantly the associated costs. It is the opinion of TUFF that providing the circumstances are clear on when and how data will be shared when the data is gathered there should be no requirements to extend the need for obtaining such persmissions on a case by

c ase basis.

Question 18.

Comments: TUFF believe the level and rights for access are about right. There may be a need for better education of the subjects especially in the levels of sharing under specific sections of the DPA. For example Sec 29 and 35

Question 19.

Comments: TUFF fully supports the ICO Framework and believes it provides a good basis for the processing and handling of personal data. It could go further with scenario based examples

Section 5: Technology

Question 20.

Comments: Technology has enabled data to be shared and stored in quantities not previously available. This in turn has led to a weakening of the processes and procedures for the sharing of data in bulk. All too often cases occur where no protection whatsoever is afforded data that is store electronically or when it is exchanged on a transfer medium It should be standard operating procedures that any personal data so exchanged is afforded a level of security commensurate with the content and quantity of data being exchanged..

Question 21.

Comments: TUFF believe that standards should be set for the storage of personal data and that the levels of protection (password/encrypted) shouldbe developed and published by the ICO. This however should NOT entail additional expense for data processors but incorporate existing processes and operating system where appropriate.

Question 22.

Comments: There is a clear need to be able to "model" data so as to be able to continue to provide levels of services comensurate to what is required. In such cases the anonymisation of data is clearly required. However TUFF believe that not sufficient guidance is given or is available from the ICO and that this aspect of data management couldbe improved upon

Section 6: International comparisons

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments: Often public attitudes differ from country to country. An example of this was when the UK Mobile Phone Industry established a database containing mobile

phone International Mobile Equipment Identifiers (IMEI). The purpose of the IMEI database was to enable UK networks to exchange this information and thus be in a position to block those equipments that had been identified as having been lost or stolen by their owners. Germany on hearing of this project argued to begin with that such data storage was against the second principle as it was personal data. The UK took the view that this was not so as the IMEI simply referred to a piece of equipment (in this case a mobile handset) and in no way on its own identified any living person. Eventually the argument that the UK put forward was accepted and the process of blocking mobile handsets in this way has now been taken up in a number of countries including Germany.

Section 7: Additional questions

Question 27.

Comments:

Question 28.

Comments:
