Identity unmasked: the hazards of flawed anonymisation

By Christine Rinik
University of Winchester

Personal data is routinely provided by unsuspecting individuals to a variety of third parties. In some cases the information is required such as when completing a loan application, whilst in other cases it may be voluntarily disclosed on sites such as LinkedIn or Facebook. The ability of computers to store, compile and sort this data has led to a huge business in "personal data." Legislation to protect the individual has attempted to classify what constitutes "personal data" so as to restrict disclosure of such information without consent. To facilitate disclosure of some "private data" an exception arises in the case of "anonymised" data where the individual cannot be identified by the information disclosed. However, the development of this exception has led to significant issues.

Following an information request to the Financial Services Authority by Efifiom Edem, the FSA refused to provide the names of its junior employees who had dealt with the matter identified by Mr Edem. (*Efifiom Edem v Information Commissioner and The Financial Services Authority; [2014] EWCA Civ 92*). In distinguishing the earlier case of *Durant v Financial Services Authority ([2003] EWCA Civ 1746)* the Court held that "A name is personal data unless it is so common that without further information, such as its use in a work context, a person would remain unidentifiable despite its disclosure." Here, Court affirmed the refusal of the FSA to disclose the names of its employees.

It would appear quite obvious to the man on the street that one's own name is "personal data." Thus the decision in *Edem* is not surprising. It is perhaps less understandable why one's name could be disclosed if it was deemed to be "commonplace" such that it could refer to a significant number of individuals, limiting the possibility that the specific individual could be identified. Whilst the intention to protect the identity of the individual is a legitimate goal, it is less clear that subjective considerations concerning the uniqueness of the data in a given population should be relevant to its potential disclosure. This paper shall argue that the approach articulated in *Edem* is untenable.

The paper will review the standards applied to the disclosure of personal data in the UK. This approach will be critically evaluated and compared to that taken in the United States where some states have adopted a more transparent system which arguably provides better protection and facilitates uniform decision making. It is argued that without clarity and uniformity, this important area of the law will fail to achieve the protection it was created to deliver. Moreover, each "error" resulting in the disclosure of "private data" creates a potential leak which cannot then be retracted— the unfortunate victim of such an error may have his or her privacy irretrievably compromised.