Science & Technology

Personal data

The logic of privacy

Jan 4th 2007
From *The Economist* print edition

A new way to think about computing and personal information

PEOPLE do not have secret trolleys at the supermarket, so how can it be a violation of their privacy if a grocer sells their purchasing habits to a marketing firm? If they walk around in public view, what harm can cameras recording their movements cause? A company is paying them to do a job, so why should it not read their e-mails when they are at work?

How, what and why, indeed. Yet, in all these situations, most people feel a sense of unease. The technology for gathering, storing, manipulating and sharing information has become part of the scenery, but there is little guidance on how to resolve the conflicts created by all the personal data now washing around.

A group of computer scientists at Stanford University, led by John Mitchell, has started to address the problem in a novel way. Instead of relying on rigid (and easily programmable) codes of what is and is not acceptable, Dr Mitchell and his colleagues Adam Barth and Anupam Datta have turned to a philosophical theory called contextual integrity. This theory acknowledges that people do not require complete privacy. They will happily share information with others as long as certain social norms are met. Only when these norms are contravened—for example, when your psychiatrist tells the personnel department all about your consultation—has your privacy been invaded. The team think contextual integrity can be used to express the conventions and laws surrounding privacy in the formal vernacular of a computer language.

Contextual integrity, which was developed by Helen Nissenbaum of New York University, relies on four classes of variable. These are the context of a flow of information, the capacities in which the individuals sending and receiving the information are acting, the types of information involved, and what she calls the “principle of transmission”.

It is the fourth of these variables that describes the basis on which information flows. Someone might, for example, receive information under the terms of a commercial exchange, or because he deserves it, or because someone chose to share it with him, or because it came to him as a legal right, or because he promised to keep it secret. These are all examples of transmission principles.

Dr Nissenbaum has been working with Mr Barth to turn these wordy descriptions of the variables of contextual integrity into formal expressions that can be incorporated into computer programs. The tool Mr Barth is employing to effect this transition is linear temporal logic, a system of mathematical logic that can express detailed constraints on the past and the future.

Linear temporal logic is an established discipline. It is, for example, used to test safety-critical systems, such as aeroplane flight controls. The main difference between computer programs based on linear temporal logic and those using other

sorts of programming language is that the former describe how the world ought to be, whereas the latter list specific instructions for the computer to carry out in order to achieve a particular end. The former say something like: “If you need milk, you ought eventually to arrive at the shop.” The latter might say: “Check the refrigerator. If there is no milk, get in your car. Start driving. Turn left at the corner. Park. Walk into the shop.”

Dr Mitchell and his team have already written logical formulae that they believe express a number of American privacy laws, including those covering health care, financial institutions and children's activities online. The principles of transmission can be expressed in logical terms by using concepts such as “previously” and “eventually” as a type of mathematical operator. (They are thus acting as the equivalents of the “plus”, “minus”, “multiply” and “divide” signs in that more familiar system of logic known as arithmetic.) For example, the Gramm-Leach-Bliley act states that “a financial institution may not disclose personal information, unless such financial institution provides or has provided to the consumer a notice.” This is expressed as:

> IF send(financial-institution, third-party, personal-information)
> THEN PREVIOUSLY send(financial-institution, consumer, notification)
> OR EVENTUALLY send(financial-institution, consumer, notification)

According to Dr Nissenbaum, applying contextual integrity to questions of privacy not only results in better handling of those questions, but also helps to pinpoint why new methods of gathering information provoke indignation. In a world where the ability to handle data is rapidly outpacing agreement about how that ability should be used, this alone is surely reason to study it.

Back to top »