Charles D. Raab & David Mason

PRIVACY, SURVEILLANCE, TRUST AND REGULATION

Online privacy: implications of a Canadian case study

The paper presented in this issue as part of the series on Privacy, Surveillance, Trust and Regulation is both disheartening and challenging as far as the protection of privacy online is concerned. Ana Viseu, Andrew Clement and Jane Aspinall's Canadian respondents in their 'Everyday Internet' project case-study are passive or resigned in the face of what privacy advocates would argue are serious invasions of privacy. These members of the public are often annoyed by the argument that they should be concerned with 'privacy' as defined by those who are actively involved in high-level policy debates. The authors acknowledge that a case study of a few individuals cannot be decisive in gauging public attitudes, but there is ample survey evidence in many countries that shows that there are a great number of people who share the views of these Canadians. Viseu and her colleagues, however, point up the extent to which people simply do not know enough about what happens to their personal data, so their complacency is not surprising when they consider the benefits they feel they gain through online transactions, and when they believe that they can adopt coping strategies to minimize whatever privacy dangers they think there might be. Such ignorance may not be bliss, but for those who are understandably bemused by the abstract concept of 'privacy' and simply want to negotiate their way in 'cyberspace', it seems to suffice.

If this is the situation for a large proportion of the population, it poses several challenges. For researchers, it opens a new page in the research agenda, for too little is known about the sources of these attitudes and how they vary across populations and categories of persons. The authors structure their argument around three overlapping 'moments' in the online experience: sitting in front of the computer in private or public spaces, and the difference that makes to one's trust; the process of giving personal information online, and the knowledge and attitudes that are brought to bear upon one's decisions and strategies for disclosure; and the aftermath of the disclosure, in terms of the legal other policy instruments that are in play to protect privacy, and the rights and responsibilities that are the main subject of privacy discourse amongst

Information, Communication & Society Vol. 7, No. 1, March 2004, pp. 89–91
ISSN 1369-118X print/ISSN 1468-4462 online
http://www.tandf.co.uk/journals DOI: 10.1080/1369118042000208915

advocates and academic writers. The authors contend that much more light needs to be shed on the first two 'moments' in order to engage policy strategy more closely with people's experiences, to grapple with their low level of knowledge, and thus to make privacy policy more effective.

This then poses a challenge to the privacy 'movement', which Viseu and her co-authors see as missing the point by not understanding what people are and are not concerned about, and therefore by not seeking solutions based on that understanding. The conception of 'privacy' as only an individual value does not help. The authors argue that the 'nothing to hide, nothing to fear' attitude may be sustained by an ignorance, which those involved in shaping policy should aim to dispel, not just by harping on 'fair information practices' but by promoting greater transparency in the way these are put into effect online when people, such as the case-study respondents, enter the first two 'moments' of a transaction. If people are fed up with all the talk about 'privacy' and 'Big Brother', then '[f]or privacy advocates, the next great challenge will be to counter this backlash'.

Whether, and how, this challenge is being met would itself be a subject for further systematic and comparative research investigation, ideally carried out by a combination of committed insiders and critical outsiders. We know too little about the privacy 'movement' and its 'advocates': how they develop as a network, or miss opportunities; what their conceptual framework takes in, or leaves out; how they deploy their resources in the policy process, or fail to; and how other policy-makers think about and interact with them, or ignore them.

Charles D. Raab is Professor of Government in the School of Social and Political Studies at the University of Edinburgh. He has published books, journal articles and contributions to edited volumes on information policy, including the formation and implementation of regulatory policies and regimes for privacy protection and public access to information. He is co-author (with C. J. Bennett) of the book *The Governance of Privacy: Policy Instruments in Global Perspective* (Ashgate, forthcoming). His ESRC-funded 'Virtual Society?' project investigated the shaping of the UK regulatory system for data protection in the context of European and global changes in the factors and concepts that currently affect the protection of privacy and personal data. He co-authored a report for the European Commission on the adequacy of data protection in non-EU countries and is currently involved in a research project on the implications of geographic information systems for privacy, identity and boundaries, under a grant from the National Science Foundation (USA). He is also researching into e-government and e-democracy. He served on the Advisory Board for the UK Government's Cabinet Office (Performance and Innovation Unit) report *Privacy and Data-Sharing: The Way Forward for Public Services* (April 2002). *Address*: School of Social and Political Studies, University of Edinburgh, Edinburgh EH8 9LL, UK. [email: c.d.raab@ed.ac.uk]

David Mason is Professor of Sociology at the University of Plymouth. He has recently completed a project, under the ESRC Virtual Society? Programme, entitled 'Technology, Work and Surveillance: Organisational Goals, Privacy and Resistance' (L132251036). *Address*: University of Plymouth, Plymouth, PL4 8AA, UK. [email: d.mason@plymouth.ac.uk]