ISBN 978-92-64-04886-7
Focus on Citizens
Public Engagement for Better Policy and Services
© OECD 2009

PART III

Chapter 29

The Privacy Implications of Public Engagement

by
Malcolm Crompton, former Privacy Commissioner of Australia 1999-2004,
and Managing Director, Information Integrity Solutions P/L

Is there a problem with privacy and what's so different about government?

"Who said it? Why did they say it? Where do they live? How did they vote last time? What are their interests and concerns?"

No, this is not from the film "The Lives of Others", George Orwell's "Big Brother" or even Ben Elton's recent book "Blind Faith".

It's the kind of questioning an elected politician and candidate in a modern democracy is expected to answer and record in the databases of their political parties' after every contact with constituents who visit their electorate office or phone in. Political parties are the most comprehensive, aggressive direct marketers on the planet. In some democracies, they even have special laws that allow them to collect more personal information from more sources than any other civilian organisation in their society and then keep it secret from their citizens.

The operations of political parties are supposed to be separated from those of government in a strong democracy. However, lines blur and more importantly, the citizenry does not always know where the boundary lies or even believes there is one. More importantly, this is a case where the facts don't matter: it's perceptions that matter.

Citizen concerns about government may have increased for at least three other reasons:

- The unique power government has in society, such as the power to pass laws that require data sharing between its agencies or other governments, be they for law enforcement, national security, service delivery improvement or policy analysis.
- The lack of choice citizens may have, for example, paying taxes, updating electoral roll data, or receiving essential health, housing or welfare services, each of which may diminish the power of citizen control as a trust mechanism.
- The lack of regular contact citizens may have with some government services. This makes it more difficult for citizens to learn to trust a service through direct experience.

For these reasons and more, democracies are required by their citizens to go to great lengths to provide a secret ballot in the ultimate consultation: general elections.

In the world of Government 2.0, the difference compared with traditional government will be the increased ability to track behaviour. Whether or not it involves "personal information" no longer matters – the impact on personal lives can be the same.

Governments will have enormous opportunities to use wiki processes to develop policy, blogs and online forums to gain feedback or social networks to generate mutual assistance between citizens. Whether they will be able to do so will depend critically on assurance of anonymity when sought and fairness in treatment in all circumstances.

Social networks moved into mainstream life extremely rapidly in 2007, followed by the desire to monetise the value so created. Then came consumer reactions to initiatives that individuals found offensive or undesirable. It all showed how powerful these tools are and how much risk they create.

In short, the question is this – how can the citizen be sure that it is "safe to play"?* How can they be assured that government will be trustworthy? Within this, "privacy" or "data protection" is a key component but not the only issue.

A new frame for generating trustworthiness

In seeking to create trust, three areas emerge as critical: *control, fair risk allocation* and *accountability*. No single one of these elements matters more than the other. What makes them powerful as a frame for thinking about trust is the way they interact. They work together in a constantly changing pattern of mutual influence and support.

When individual citizens say they don't trust an organisation or demand "privacy", it is likely that these are the three things that actually concern them, even if they might not articulate it that way.

A dynamic system linking control, risk allocation and accountability

Control

First, citizens are concerned that either they will lose control over what happens to information about them or that they have insufficient control over how that information is demanded, collected and stored in the first place. Their sense of loss of control is heightened if they do not understand how organisations control any such information that they have. It is heightened a lot more if they fear new information will be used against them in their daily lives.

Risk and its allocation

The sense of unease will grow – along with the feeling that this is a game in which it is not "safe to play" – if citizens don't have enough knowledge about the risks of participating in a consultation and how the risks that do exist have been defined and allocated.

This is a very significant issue for governments. Citizens are becoming much more aware that they have been asked to shoulder an increasing proportion of risk in most parts of their lives over the last couple of decades. Will a new consultation lead to more?

Accountability

Finally, citizens are concerned that organisations which collect and use information about them, too often fail to accept full accountability. In particular, they fail to demonstrate full accountability for the way they manage risk or to accept responsibility quickly and effectively when risks manifest themselves as failures or breaches. While organisations manage failures affecting themselves with business continuity plans, the equivalent "citizen continuity plan" is often strangely missing for other stakeholders in a service provision relationship, especially the service user.

Lack of a good safety net for citizens when failure occurs is tantamount to allocating a disproportionate amount of risk to the individual, who is often least able to manage, mitigate or bear that risk compared with a government agency.

* This thinking derives from work funded by Cisco Systems. To read the full paper on "Safe to Play – a Trust Framework for the Connected Republic", visit *www.iispartners.com/Publications/index.html*.

The dynamics

These three factors are significant because they are interdependent. If issues in only one or even two of the elements are addressed, it's unlikely that the trust dimension will have been properly addressed. Sometimes they are complementary; at other times they are not. A common reaction to a perceived increased in personal risk, for example, is to demand increased personal control or anonymity. Another example is the way greater accountability can be used to reduce risk significantly. Each component must be addressed to achieve rising levels of trust.

Where to from here?

This analysis tells us one thing: governments have to act in a trustworthy way if they are to engage their citizens in meaningful consultation that is to be viewed as neither "spin" nor entrapment. The key to earning trust will be respect for individual citizens and the personal information about them through a particular focus on control, risk and accountability, viewed from the citizen perspective. When government consults through new channels that leave richer footprints, such as Web 2.0 tools, the need to address these dimensions becomes even more critical.

The final test, though, remains unchanged – old fashioned good public administration – listen to the outcomes of consultation and "say what you're going to do and do what you say" in response.

Some suggested principles

The following principles provide a practical guide for governments exploring new ways to build high trust into all dimensions of consultation and service provision:

Control

- Don't hide behind consent if the service user has no real choice.
- Be prepared to pay greater attention to mitigating citizen risks, accountability and a safety net where direct citizen control is not possible.
- Give citizens as many options as possible about how they manage their relationships in the online world. Make it possible for them to conduct these relationships as they would in the offline world if they wish to.
- Encourage a learning system. Enable people to understand and discover the capabilities and risks of a new service gradually and in a safe environment. Encourage adaptive solutions that use the "power of the edge".

Fair risk allocation

- Focus on risk for all parties, including the citizen. Identify, allocate and be clear and specific about ways to mitigate it. Align the incentives so that risk is managed by those who are best able and motivated to manage it. In particular, look after citizens when they are ill-equipped to look after themselves.
- Regularly review risk settings to make sure they evolve appropriately in line with the dynamic nature of the collaborative web environment.

Accountability

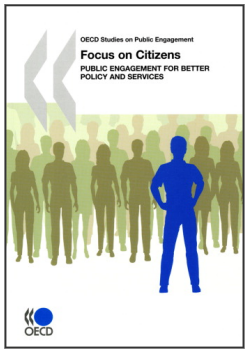
- Be prepared to be more transparent.
- Have strong internal and external audit and review mechanisms to demonstrate trustworthiness.
- Ensure that there is a good safety net for citizens when service delivery fails them in some way. Credible restitution (for example, for identify theft) is worth more than over-promising a foolproof, perfect system.

Table of Contents

Boxes

Tables

Figures



From:

Focus on Citizens

Public Engagement for Better Policy and Services

Access the complete publication at:

https://doi.org/10.1787/9789264048874-en

Please cite this chapter as:

Crompton, Malcolm (2009), "The Privacy Implications of Public Engagement", in OECD, *Focus on Citizens: Public Engagement for Better Policy and Services*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/9789264048874-32-en

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgment of OECD as source and copyright owner is given. All requests for public or commercial use and translation rights should be submitted to rights@oecd.org. Requests for permission to photocopy portions of this material for public or commercial use shall be addressed directly to the Copyright Clearance Center (CCC) at info@copyright.com or the Centre français d'exploitation du droit de copie (CFC) at contact@cfcopies.com.