Drawing lessons from disasters

Blair Stewart, Privacy Foundation New Zealand Committee member, 29 March 2020

Back in February 2019 I was honoured to be invited to deliver a lecture to a symposium to be held in Tokyo in October that year on the subject of regulating privacy in natural disasters. Unfortunately, as it turned out, the event was postponed to late-February 2020. I never got to deliver my paper due to my Kansai University hosts having the wisdom to cancel the symposium.

The topic was one that had interested me since the Cave Creek Disaster in 1995 when the Privacy Act was publicly slammed by a local police officer as "one of the biggest problems that we had on the day". During my 25 years as an Assistant Privacy Commissioner I sought to understand the interaction between disasters and privacy law and find ways to make privacy law work better in difficult conditions and ensure it didn't work against individuals' vital interests.

The Privacy Foundation NZ has kindly agreed to post my undelivered paper **Sharing and protecting personal information in natural disasters: A perspective from a former privacy regulator** to its website. The paper explains why major natural disasters impact information laws and offer suggestions for proactively addressing the challenges. It is full of examples mainly drawn from the experience gained from the Canterbury and Christchurch Earthquakes of 2010 and 2011.

The paper also outlines the background to the Civil Defence National Emergencies (Information Sharing) Code 2013 which was, for the first time, activated a week ago by reason of the declaration of a state of emergency under the Civil Defence Emergency Management Act 2002. Accordingly, there has been an automatic activation of additional legal discretion for disclosure of personal information to assist in the management of the emergency.

I offered the following conclusions in my paper[1] (slightly edited and shortened for this commentary):

Three recommended practices for sharing and protecting personal information in natural disasters

There is no single correct way to resolve the tension between the usual best practice for protecting privacy and the extraordinary circumstances that may be encountered. However, these are my three principal suggestions.

1. The basic privacy law should be able to cope with small emergencies and standard and anticipated natural disaster responses

New Zealand's privacy law has plenty of flexibility and hasn't struck significant problems with the frequent local states of emergency that have been declared over the years. Even the large Canterbury Earthquake preceding the Christchurch Earthquake did not warrant issuing a code of practice. The Civil Defence National Emergencies (Information Sharing) Code 2013 is triggered only by a declaration of a state of national emergency.

The necessary flexibility in the New Zealand law arises in various ways such as statutory overrides and the exceptions to principles for serious threats and public health and safety and the ability to grant individualised exemptions (although the latter have not been needed in any local emergencies to date). In 2013 provision was made in the Privacy Act for flexible "approved information sharing agreements" between public sector agencies.

[1] The full version of the paper may be viewed at www.privacyfoundation.nz/wp-content/uploads/2020/03/Sharing-and-protecting-personal-information-in-natural-disasters.pdf

To take an example of another law, article 6(d) of the EU General Data Protection Directive allows for processing where "necessary in order to protect the vital interests of the data subject or of another natural person".

GDPR recital 46 explains article 6(d):

> The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

Article 6(d) is an important and flexible provision. However, as the examples in the paper show, many of the useful disclosures resulting from a natural disaster, especially in the recovery phase, do not all involve "vital interests" in the sense of saving lives.

The literature includes examples of laws that have been found to be unduly restrictive in relation to reasonably foreseeable scenarios (a couple of examples are offered in the paper).

One particular issue arising from major natural disasters (and other humanitarian emergencies such as armed conflict) is the need, and the difficulty, of tracing missing persons and reconnecting them with families. The report *Privacy and Missing Persons after Natural Disasters* reviewed EU and US law in this respect and found the principal federal privacy law too inflexible in that context. By contrast, the more modern US federal health information privacy law, HIPAA, specifically addressed the issue as recounted in *Privacy and Missing Persons after Natural Disasters*:

> (4) Use and disclosures for disaster relief purposes. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

In Canada there were media reports that Federal government officials were citing the Privacy Act as a reason for not releasing the names of Canadians missing and feared dead in the Indian Ocean Tsunami disaster. One eventual response was the insertion into the Canadian private sector privacy law PIPEDA providing that an organisation may disclose personal information without the knowledge or consent of the individual if the disclosure is:

> necessary to identify the individual who is injured, ill or deceased, made to a government institution, … or the individual's next of kin or authorized representative and, if the individual is alive, the organization informs that individual in writing without delay of the disclosure.

2. Whatever approach is taken effort should be made to seek to ensure that relevant organisations or staff will be aware of the discretion to share information

Often staff in organisations believe that the privacy law prohibits them from disclosing information but are blissfully unaware of the wide discretions they may have to release information. It is too late to try to start educating staff about exceptions to a privacy rule once a major natural disaster strikes.

When the Privacy Commissioner issued the temporary code of practice within 48 hours of the Christchurch Earthquake a difficulty was faced in arranging to notify organisations and staff that might benefit from it. The code could be posted online but telecommunications had been knocked out. A media release could be issued but the news media were busy with far more engaging stories from the disaster. The code was disseminated through the officials' committee that coordinated the government's disaster response. The Privacy Commissioner was not in a position to assess how effective that was. In a later review, it was clear that even 7 weeks later many front-line staff who might have benefited from the code's discretions were unaware of the code's existence.

Learning from this experience the Privacy Commissioner issued, two years later, the Civil Defence National Emergencies (Information Sharing) Code 2013. This code would come into effect in the event of a declaration of national emergency. Its terms were similar to the temporary 2011 code but a key difference was that its existence was known to agencies in advance and could be factored into staff training and contingency planning.

3. Consideration might usefully be given to special discretions for information sharing in extraordinary circumstances of a major natural disaster

As a privacy advocate, I would not propose suspension of a privacy law in a time of crisis. That could leave human rights unprotected unnecessarily and undermine trust in public institutions. However, allowing additional, though still limited, additional discretion for sharing information in an emergency is a proportional approach that can be reconciled with human rights norms.

This paper has described how the Privacy Commissioner has taken that step for declared national emergencies. The Australian Parliament did much the same thing in an amendment to their privacy law several years earlier. Such an approach will not suit some legal traditions or even be necessary depending on how their general privacy law copes with the issues.

If this approach is taken it is essential that some limits be imposed and safeguards included. My recommendations are that:

- ordinary law should continue to apply where possible;
- where special delegated legislation is warranted, the original law be reinstated as soon as feasible;
- there should be monitoring to ensure that the need for special arrangements continues and that the delegation is working as intended;
- any derogations from usual law and rights should be proportionate to the need and that appropriate safeguards be in place;
- temporary delegations of power should be subject to review after the national emergency is over; and
- results of reviews of the exercise of special powers should be made transparent.

Each of these principles was scrupulously applied in relation to the Commissioner's 2011 code.