HRMI Data Security Policy

HRMI collects two types of sensitive information as part of our Civil and Political Rights metrics development. These two sets of data are stored separately:

- Information about potential expert survey respondents and the people who nominated them.
- Survey responses to our annual expert survey.

This policy – updated in 2020 following a security audit conducted by a cyber-security firm – explains our security steps for each.

1. Names and contact details of potential survey respondents

This information is collected in two stages. First, human rights practitioners may be nominated (via a secure online form) for inclusion in the survey by HRMI appointed Ambassadors who are our local partners, people at our trusted partner organisations, and in some cases, from existing survey respondents. Nominees are then asked whether they wish to participate in the survey. If they agree, they provide their name and email address via a secure online consent form. Key features of our security policy are:

- All online forms are hosted on the HRMI website which has an SSL certificate and is secured by https. This means that the information is secure (encrypted) in-transit.
- Names and emails submitted via the consent form are sent directly (encrypted) to our Client Relationship Management (CRM) software. The cloud-based CRM is certified to all relevant security ISO standards including 27001, 27017 and 27018, which ensures all information is captured, managed and retained in an encrypted fashion. Access to the CRM is restricted to a small team of New Zealand-based HRMI staff.
- HRMI uses this information to send a unique link to HRMI's online expert survey to each of these potential survey respondents.
- The names of people who are nominated for inclusion in the survey, but who do not complete the consent form, are not added to the CRM database, and all nomination details are deleted after data release each year.

2. Survey responses

The survey is hosted on the Qualtrics website which has an SSL certificate and is secured by https. This means that all information entered and transmitted is encrypted. IP addresses are *not* stored. Access to the Qualtrics response data is restricted to a small team of HRMI staff based at the University of Georgia's (UGA) Center for the Study of Global Issues (GLOBIS).

The main potential risk to survey respondents is that if their email is hacked or they are under surveillance, hostile agents may see they are communicating with HRMI and know they are *potentially* contributing to our civil and political rights metrics.[1] But they would likely not be able to access the survey information submitted itself. The only exception to this would be if the respondent is under surveillance which includes keylogging, for example, in which case it is possible that some of the respondents' entries in the survey could be insecure. If this is something to be concerned about, we would strongly encourage respondents to fill out the survey using trusted, non-shared devices over which the respondent has complete control, along with following the other guidelines (listed on our website) for protecting themselves from online surveillance.

The survey responses that HRMI receives via Qualtrics are unidentified. i.e. we do not link responses to individual survey respondents. However, some of the qualitative responses provided might *potentially* be able to be used to identify some respondents in rare cases. Therefore we have identified 3 different levels of data security from 1 (confidential) to 3 (public).

- 1 - **Confidential**: the initial raw data received via Qualtrics by HRMI staff at UGA contains all qualitative and quantitative responses. These data are deleted from the Qualtrics server after processing. Only people who have security training and who are conducting relevant research have access. All information that could potentially identify respondents is ultimately destroyed.
- 2 - **Research Data**: Fully de-identified survey responses – to be used in research and to calculate HRMI metrics – requires no special security as the data are fully anonymous. These data may be shared online as replication data with HRMI publications.
- 3 - **Public**: Aggregated data are published on the HRMI Rights Tracker as HRMI metrics and downloadable directly from the HRMI website.

[1] To mitigate this risk, we provide information on how potential survey respondents can protect themselves from on-line surveillance.