

Small World News

This case study examines how Small World News used FrontlineSMS for election monitoring and the associated data protection and security vulnerabilities, threats, risks and actions taken to reduce risks.

Project Description	Small World News used FrontlineSMS in a Middle Eastern nation to allow residents and citizen journalists to report their election experiences and concerns.
Vulnerabilities	<ul style="list-style-type: none">• Lack of encryption for SMS messages• Use of government-controlled Mobile Network Operator (MNO)
Threats	<ul style="list-style-type: none">• SMS messages intercepted by a third party or unauthorized user• SMS messages and citizen reporter information accessed by the government
Risks	<ul style="list-style-type: none">• Sensitive information contained in SMS viewed or changed• Citizen reporter physically tracked by the government
Risk Reduction	<ul style="list-style-type: none">• Sanitization of reports• Use of numeric digits to represent incident types• Separate numbers for trained and untrained reporters• Use of a firewall and secure connections to protect stored information

FrontlineSMS and Small World News

Small World News connects citizens in crisis areas and conflict zones with the international community. The project empowers global citizens to share their stories by providing them with citizen journalism tools.

Small World News used FrontlineSMS to monitor an election in a Middle Eastern nation by enabling citizens to voice their thoughts or concerns via SMS. Examples of reports included problems encountered at the polls and unusual or illegal activity. Small World News also used Ushahidi, an online geographic heat-mapping platform, to track the locations of the incoming SMS messages.

Small World News trained a number of citizen reporters on the types of incidents to report and the proper reporting process. The project also allowed the general public to send reports.

Data Protection Concerns

A major concern for Small World News was the lack of encryption when SMS messages were sent by the reporter. A third party could have used basic technology to launch a man-in-the-middle attack and monitor or modify the SMS reports the project received. The MNO used for the project was controlled by the government, which allowed the government to store and monitor the sensitive information sent by the reporters to Small World News. This was a concern for Small World News because citizens sending in reports of unusual or illegal activity could have been easily identified or physically tracked by the government. To date, Small World News has not not experienced any of the risks associated with the lack of SMS encryption or the use of a government-controlled MNO, but recognized these concerns as vulnerabilities.

Lastly, the validity of the messages received was a concern for Small World News. If false or exaggerated information was provided, there was the possibility that it would be included in a public report published by Small World News, and the reputation of the project could have been damaged.



Actions to Protect Data

To reduce the risk of reporters being identified and being physically tracked, Small World News trained a number of reporters to send reports using numeric digits to represent a type of incident. This type of reporting can mask activity from being monitored, and is harder for a third party to read.

To reduce the risk of false information being processed, Small World News sanitized all incoming information to validate the accuracy of the report. Phone numbers of trained reporters were stored in a database and were automatically approved or hidden if the information was for internal use. Reports received from trained monitors were processed using a script to determine the incident type that maps to the numeric code. Small World News used an unpublished phone number to receive information from trained reporters to maintain a high quality of reporting.

To validate reports received by the public, a team member who was familiar with the area from which the report originated reviewed the report. They could immediately discard reports that mentioned a location that did not exist or an event that was not likely for the area. If a report was questionable, a team member was deployed to verify the report. Individuals' names, phone numbers or other identifying information was usually removed from the report to protect the reporters.

To reduce the risk of sensitive information being viewed by an unauthorized user, all information was stored in secured databases behind a firewall. Additional measures, such as an early warning system, were taken to detect potential attempts to compromise the system. Sensitive data was regularly backed up to an offline database and sanitized, so that if the system is compromised there was little personally identifiable information and only unprocessed reports would be vulnerable. All connections for administration purposes were performed over SSL or used a secured connection such as a proxy or VPN.

Conclusion

It is very difficult to mitigate the risks associated with the transmission of SMS messages in plain text, however, the use of numeric digits to represent incidents can protect the message content even if it is intercepted. The use of separate phone numbers for trained and untrained reporters helped to maintain a high quality of information.