THE DIGITAL SECURITY OF CANADIAN JOURNALISTS FOR FREE EXPRESSION (CJFE)

EXECUTIVE SUMMARY

This report assesses the digital practices and vulnerabilities involved in the Journalists in Distress (JID) program that is operated by Canadian Journalists for Free Expression (CJFE), one member of a, global network of organizations that provide humanitarian assistance to journalists and other media workers around the world who are persecuted because of their work. Both CJFE's JID program and the global network face the challenge of adapting to the rapidly changing digital contexts in which they work.

Given its comparatively small size for a free expression organization with a transnational mandate, assessing the digital practices and vulnerabilities of CJFE's JID program provides a baseline for the digital components that can be used in this type of emergency assistance program, and the level of digital security that can be achieved as a result. All types of digital practices employed in the course of CJFE's JID programming are documented, including the various hardware and software used in this work. They are divided into three channels: the internal communications within the organization, the communications between CJFE staff and applicants to the program, and communications with network and non-network members related to JID work. In Part 1, these three channels are presented comprehensively; in Part 2, they are evaluated for the digital security strengths and vulnerabilities they afford CJFE's JID program.

Part 1 begins with an overview of CJFE's origins, staffing, and the achievements of its JID program. The internal communications involved in its JID program are discussed by mapping the stages and actors involved in the program's decision-making process and the modes of communication employed, as well as the various software and web tools that are used during this communication. Staff communication with applicants to CJFE's JID program are discussed, including the types of information collected in its application form and where journalists are contacting CJFE from. The communications between CJFE's program staff and the members of the global network are described, including a historical account of how its primary mode of communication has changed. The many different types of non-network members that are contacted by CJFE staff in the course of its JID work are also discussed, as well as the reliance on email for these interactions. Part 1 ends with a summary of the many hardware devices involved in CJFE's JID program and the state of their security.

Part 2 provides an overview of the strengths and weaknesses that are present in CJFE's digital security practices (laid out in Part 1), and then each component is discussed in more detail. Overall, CJFE's digital practices are a mix of strengths and weaknesses that often (and not surprisingly) accompany limited resources, partial knowledge, and heavy workloads. However, CJFE has also creatively fashioned a number of methods for increasing the security of its JID data despite its limited resources; this is especially reflected in the hardware and software that the staff use as part of their emergency assistance work.

The primary finding from the analysis in Part 2 is that even when practices and technologies are implemented which have the capacity to improve digital security, staff behaviours and risks are present that can compromise any added security. This is doubly important to realize in order to avoid being lulled into a false sense of security—in other words, by believing the existing security practices and technologies are working as they are supposed to while not realizing that other vulnerabilities are still in effect.

The digital security strengths and weaknesses indicate that in order to safeguard the communications and information of CJFE's JID program, staff must understand that practices and technologies can be made more or less secure. In many cases, it is the human behaviours and decisions that jeopardize digital security, rather than technical flaws in the technology being used. Digital security is not a one-time achievement that need never again be considered a concern or challenge; rather, it must be continuously maintained, reevaluated, and upgraded. In addition, there is a handful of changes taking place or on the horizon at CJFE that will present new digital security challenges for the staff to address. However, these challenges also present opportunities for the staff to begin new conversations about their digital security, and to plan new ways to fill any existing or emerging gaps.

AUTHOR

Taryn Blanchard is the Programs Coordinator at Canadian Journalists for Free Expression (CJFE), a Toronto-based non-profit organization that works to promote and protect freedom of expression and access to information in Canada and around the world. She is also a PhD candidate in the Department of Anthropology at the University of Toronto, where she researches free expression advocacy in today's digitally mediated world, with a focus on how transnational human rights networks are built and used strategically by activists and individuals at risk.

To contact Taryn, please email tblanchard@cjfe.org or taryn.blanchard@utoronto.ca.

OPEN TECHNOLOGY FUND

CJFE