Researcher–participant confidentiality now a formal concept in Canadian law

The successful quashing of a search warrant for confidential research records has changed the landscape for protecting research participants in Canada, says a research confidentiality expert. John Lowman, a criminology professor at Simon Fraser University in Burnaby, British Columbia, says the court decision makes researcher–participant confidentiality privilege a formal concept in Canadian law. However, the privilege won't apply automatically to all confidential data; the ruling from Quebec Superior Court underscores that it must be argued on a case-by-case basis.

The pivotal case began in late May 2012, when an international manhunt was underway for Luka Magnotta, the porn actor suspected in the gruesome, videotaped murder of a Concordia University student in Montréal, Quebec. With the Web awash in photos of Magnotta, a man contacted police and told them that five years earlier, when he was a research assistant on a Social Sciences and Humanities Research Council–funded study of escorts, he had interviewed the alleged murderer. University of Ottawa criminologists Chris Bruckert and Colette Parent led that study, but when Montréal police asked Bruckert if Magnotta had been interviewed, she said she didn't know.

"In fact, there was no way I could have known," she told *CMAJ*. To protect the privacy of research participants working in the sex trades, Bruckert and Parent used strict confidentiality protocols, including asking participants to choose pseudonyms — Magnotta chose "Jimmy" — and having their research assistants sign the pseudonyms to consent forms, to guard against anyone identifying participants based on handwriting. After an interview was taped, transcribed and stripped of obviously identifying information, they sent it to the participant to delete other identifying details. Once the participant returned the transcript, the team destroyed the participant's email address, along with the connection between the name, email address and pseudonym.

Paul Jones

University of Ottawa criminologists Chris Bruckert (above) and Colette Parent, maintain that their research on sex workers would be impossible without confidentiality.

Undeterred, police told Bruckert they would take legal steps, including a search warrant, to obtain the interview.

Bruckert contacted the Canadian Association of University Teachers (CAUT) where Executive Director Jim Turk hired Peter Jacobsen, a lawyer known for defending journalists who are pressed to divulge their sources. Bruckert sent the digital audiotape of the interview and the 68-page transcript to Jacobsen's Toronto office. Police seized the materials there, but took them in a sealed package, because of the legal move to quash the search warrant on the grounds that it would violate the researchers' promise of confidentiality.

By then, Magnotta had been arrested in Berlin, Germany. Later he wrote an affidavit stating that he gave an interview as "Jimmy" in a study at the University of Ottawa, that he was assured the interview would be private and confidential, and that he wanted it to remain so.

To Bruckert, the threat was clear: her research on sex workers would be impossible without confidentiality. But the issue had been tested only once before in Canada. In a 1994 coroner's inquest in Vancouver, BC, a master's student was subpoenaed to testify about confidential interviews with individuals who assisted suicides among people with HIV/AIDS, but after he refused to answer questions, the coroner ruled that the student's communications with his research participants were privileged so his refusal to answer questions was not in contempt of court.

As Bruckert and Parent worked to prepare their case, CAUT negotiated with the university, seeking its support of the researchers, but University of Ottawa President Allan Rock wrote Turk that the university would not pay legal costs "in

© 2014 Canadian Medical Association or its licensors

the context of criminal proceedings." Members of the university's research ethics boards also pressed for support for the professors, writing Rock that a board had approved the research on condition of the participants' confidentiality, and months later, university administrators agreed to cover about half CAUT's expense, or $150 000.

The hearing took place in April 2013 before Justice Sophie Bourque of Québec Superior Court. Her 37-page decision issued Jan. 21, follows a legal framework known as the Wigmore criteria, a four-step analysis to determine if a particular communication should be protected against disclosure. The case hinged on whether the public interest in obtaining the "Jimmy" interview for the investigation and suppression of crime outweighed the interest in what Justice Bourque described as "the free flow of accurate and pertinent information," which could dry up without a reliable promise of confidentiality. She broke the seal and reviewed the interview transcript privately, but did not share its contents, writing that its relevancy to the charges against Magnotta or to a "not criminally responsible" defence was "minimal at most and marginal." Bourque quashed the search warrant, concluding that "the confidential interview is covered by the researcher–participant confidentiality privilege and … it should not be disclosed."

The Crown had until late February to appeal the decision but as of press time (Feb. 6) the case had already prompted rethinking of researchers' duties. New guidelines at the University of Toronto, for example, list principles to be followed in "research where external pressure to disclose is reasonably foreseeable" and the federal Interagency Advisory Panel on Research Ethics told *CMAJ* it would issue a new interpretation of the duty of confidentiality in the next two months. — Miriam Shuchman, Toronto, Ont.

CMAJ 2014. DOI:10.1503/cmaj.109-4717

New tools to improve safety of electronic health records

The US government has created a set of guides and tools to help health care providers more safely use electronic health records (EHRs). *The Safety Assurance Factors for EHR Resilience (SAFER) Guides* — which include self-assessment checklists, practice worksheets and recommended practices — were released by the US Department of Health and Human Services on Jan. 15.

"With the release of these guides, stakeholders now have ready access to additional evidence-based knowledge and practical tools to optimize EHR safety," Dr. Jon White, director of the Health Information Technology Portfolio for the Agency for Healthcare Research and Quality, said in a press release. "Consistent with the Health IT Safety Plan, health care providers and those who support them will use these guides to develop a culture of safety, shared responsibility, and continuous improvement around health IT."

Nine areas are addressed by the *SAFER Guides*, including organizational responsibilities, patient identification, clinical communication, test results review and follow-up, system configuration and contingency planning.

A contingency plan is necessary when an EHR system has an unexpected shutdown, which could be due to software failure, hardware malfunction, power outage or any number of unplanned events.

Wavebreak Media/Thinkstock

The United States government has created a set of online guides and tools to help health care providers more safely use electronic health records.

Many problems and delays can arise when electronic records become unavailable, says Dean Sittig, a professor in the School of Biomedical Informatics at the University of Texas Health Science Center at Houston.

It can become difficult to register patients, obtain test results from labs, communicate between departments and bill for medical services, to name but a few common problems. And not all hospitals are adequately prepared to function well during an outage.

"The hospitals where there have been downtimes in the past fare better than those that haven't," says Sittig. "For some reason, people don't want to learn this lesson when it happens to their neighbours."

To prevent EHR downtimes, health care providers should duplicate all critical hardware, have generators support their electronic systems during power outages and implement comprehensive testing and monitoring strategies. If a shutdown still occurs, there should be paper forms available, polices in place to ensure accurate patient identification and a communication strategy that doesn't rely on an electronic system.

"The recommended practices in the *SAFER Guides* are intended to be useful for all EHR users, developers, patient safety organizations and others who are concerned with optimizing the safe use of Health IT," states the guides' website. — Roger Collier, *CMAJ*

CMAJ 2014. DOI:10.1503/cmaj.109-4715

© 2014 Canadian Medical Association or its licensors