Delimiting Digital Searches: Observations on Irish Law and Reform

Dr TJ McIntyre

Associate Professor, UCD Sutherland School of Law

Consultant, FP Logue Solicitors

Chairperson, Digital Rights Ireland

Outline

- Digital searches are different
- Irish search warrants don’t account for these differences
- Cases are beginning to expose the resulting problems
- Current proposals to reform search warrant powers do not address these issues

Digital searches are different

- “In 1926, Learned Hand observed that it is “a totally different thing to search a man’s pockets and use against him what they contain, from ransacking his house for everything which may incriminate him.” If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.”

- *Riley v. California,* 573 U.S. 373 (2014), *per* Roberts CJ
- Restricting search incident to arrest

- “The privacy interests implicated by computer searches are markedly different from those at stake in searches of receptacles such as cupboards and filing cabinets. Computers potentially give police access to vast amounts of information that users cannot control, that they may not even be aware of or may have chosen to discard and which may not be, in any meaningful sense, located in the place of the search.”

- *R v Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657, *per* Cromwell J
- Restricting search of computers/phones not specifically mentioned in warrant

Irish search warrants don’t account for these differences

Not all search powers address data, but those that do are incredibly expansive

- The nature of the power depends on the particular crime being investigated
  - “[C]urrent statutory powers to issue search warrants constitute an unwieldy collection of disparate provisions which have been developed in a piecemeal fashion over the past two centuries.”
    - Dermot Walsh, *Criminal Procedure* (Thomson Round Hall, 2002)
  - There are distinct *production order* powers which are not as problematic
- Most search powers which specifically deal with data follow the model of the next slide

s.48 Criminal Justice (Theft and Fraud Offences) Act 2001

(5) A member of the Garda Síochána acting under the authority of a warrant under this section may—

(a) operate any computer at the place which is being searched or cause any such computer to be operated by a person accompanying the member for that purpose, and

(b) require any person at that place who appears to the member to have lawful access to the information in any such computer—

(i) to give to the member any password necessary to operate it

(8) In this section…

"computer at the place which is being searched" includes any other computer, whether at that place or at any other place, which is lawfully accessible by means of that computer;

Implications of s.48?

- S.48 does not have a proportionality requirement for the issue of a warrant, or use of powers under the warrant
- *Every* warrant under s.48 includes a power to examine, operate and seize computers and compel production of passwords by any person present
- There is no provision addressing the issue of self-incrimination
- The reference to “any other computer, whether at that place or at any other place, which is lawfully accessible by means of that computer” permits remote searches, including of cloud services, including in other jurisdictions
  - Comity issues?

- Failure to hand over a password “without excuse”, there and then, is a criminal offence
- This seems to require disclosure of passwords to remote computers and cloud services also
- S.48 prohibits seizure of privileged material – but doesn’t address the issue of screening of seized material
- There is no provision addressing other sensitive material – notably material relating to journalists’ sources

Cases are beginning to expose the resulting problems

CRH v Competition and Consumer Protection Commission [2017] IESC 34

- Seizure of all emails belonging to a CRH executive, including emails unrelated to the business of the undertaking being investigated
- High Court & Supreme Court held that CCPC was not entitled to seize the records outside the scope of the investigation
- What should be done with the mixed seized data?
  - Statutory power did not provide for any sifting process for determining relevance or addressing privacy interests
  - Courts left it to the parties to agree a process for doing so

Corcoran v Commissioner of An Garda Siochana [2020] IEHC 382

- Seizure of journalist's mobile phone on foot of a search warrant
  - Aiming to identify who tipped off journalist about an upcoming attack on security men carrying out an eviction
  - To obtain photos/video of those carrying out the attack
- Legislation did not provide for an assessment of "journalistic privilege" issues at the point of issue of the warrant
- Court declines to "read in" an *inter partes* hearing or similar safeguard into the legislation, which provides for *ex parte* applications only
- Court sidesteps issues of the validity of the warrant by finding that "journalistic privilege" would not apply in the circumstances in any event
- Court orders that examination of the phone be limited to information from the time period around the attack, but without identifying any statutory basis to do so

No (?) prosecutions for failure to disclose passwords

However, prosecution for withholding passwords is generally not done due to the right against self-incrimination. Surveillance warrants can be obtained under the Criminal Justice (Surveillance) Act 2009 to monitor computers that use encryption, and this can overcome difficulties in serious criminal cases where it is known that encryption is being used and passwords will not be handed over.

- "7th Round of Mutual Evaluations on Cybercrime – Ireland" (2017)

Current proposals to reform search warrant powers do not address these issues

- 2015 Law Reform Commission Report on Search Warrants and Bench Warrants recommends extending s.48 type powers to all offences
- But:
  - Does not include any empirical assessment of use of these powers
  - Does not address the issues we identified earlier

Garda Síochána Powers Bill 2021

- Head 16 would extend the s.48 model to all search warrants
- It goes further than s.48 by clarifying that:
  - “the person searching may use passwords or other information that they have found themselves during the course of the search- for example passwords found on mobile phones- to access other devices.”
- Similarly, the Heads of Bill explicitly envisage remote searches:
  - “Paragraph (e)(iv) includes a power that is currently provided for under section 37 of the Competition and Consumer Protection Act 2014 to compel the production of material under a person’s power or control, but with the qualification that they must be accessible to the search site- as a search warrant is primarily for the search of a place.”

- There is a carve-out in relation to privileged material (Head 19)
- There is explicit power to seize “mixed” material (Head 20)
  - But no provision for how that material should be dealt with after it is seized!
  - Heads of Bill: “It is intended that this is a matter that could be addressed in the codes of practice”
- Codes of practice would have disciplinary effect only
- The Bill continues the practice of “self-service search warrants” in cases of urgency (Head 21)
- In some cases the CCPC/ODCE could seek warrants “even where no offence is suspected”.

Thank you.
Questions/comments?

Dr. TJ McIntyre

contact@tjmcintyre.com

Twitter: @tjmcintyre