The High Court of Australia Paves the Way for the Use of "AN0M" Evidence – and Validates Global "Outsourcing"

Frederick T. Davis[1]

On October 8, the High Court of Australia issued a ruling entitled *CD v. Commonwealth of Australia* that validated legislation rapidly adopted by the Parliament to remove evidentiary obstacles to the prosecution of drug dealers and other alleged criminals who had been caught in a massive international "sting" using the so-called "AN0M" technology, known in Australia as Operation Ironside. The outcome paves the way to the likely conviction of hundreds of apparent malefactors. The decision, which approves the Parliament's retroactive intervention in evidence issues pending in a criminal case, is fascinating on its own and noteworthy in the context of the rapid globalization of crime and investigation, as well as the possibility of "outsourcing" evidence that is inadmissible in one country for use in another.

The AN0M Saga

"AN0M" is the name given by the Federal Bureau of Investigation (FBI) to a high-tech device that it developed in 2018, based on cryptographic technology that permitted its users to communicate securely. Building on techniques invented by a cooperating informant, the FBI created a communication platform that it passed on to unsuspecting underworld "influencers" who, in turn, urged their partners-in-crime to use it. The centerpiece was a normal-looking smartphone, called AN0M, that communicated only – and with a high degree of encryption – in a "closed loop" with other AN0M devices. From the point of view of the users, it worked wonderfully – except for the fact, unbeknownst to them until the story broke in June 2021, that the FBI had included a "back door" such that all of the literally millions of communications shared by its users were transmitted to FBI-designated authorities. The AN0M devices sold slowly at first, but in 2020 and 2021, somewhat similar programs known as EncroChat and SKY ECC were unmasked, and many of their users turned to AN0M. Ultimately, some 11,000 happy users purchased and actively used the devices, and generated tens of millions of often incriminating communications, sometimes with remarkable additions such as photos of actual narcotics, laundered money, and the like. The details of this caper are fascinating and were summarized by Joseph Cox in a 2024 book called Dark Wire: The Incredible True Story of the Largest Sting Operation Ever.

The story broke in June 2021 and led to coordinated mass arrests in sixteen countries around the world.

Was AN0M Evidence Admissible?

While imaginative and wildly successful, the AN0M experiment faced a big challenge: the fruits of its use almost certainly violated the laws of many countries. The core problem is that the configuration of the devices amounted to massive electronic eavesdropping -- a wiretap – where in general no pretense was made to obtain a prior judicial probable cause finding. The FBI asserted that it only sold the device to "criminals," which was surely their intent, but of course, most laws protecting against eavesdropping are not satisfied by the untested, unreviewed conclusion of a police officer. The FBI claims that it "geo-fenced" the AN0M devices to exclude communications to/from the United States (U.S.). There appears to have been one instance where AN0M evidence led to a prosecution in the U.S., based on evidence obtained outside the U.S.; an argument by the defense that the use of non-U.S. police programs should be excluded was denied, and the defendants pleaded guilty.

To develop the program and achieve broader impact, the FBI reached out to other friendly countries, shared the new technology with them, and encouraged them to use it under their own criminal procedures. Many individuals were caught up in this dragnet in Europe and faced prosecution there, with mixed results. At least one court (in Germany) refused to allow the AN0M-based evidence to be used, reasoning that the procedures were illegal in the country of its birth (the U.S.) and that the court could not participate in an effort to "outsource" the investigation. Several such cases continue to work their way through the appellate process.

AN0M in Australia: Operation Ironside

[1] Frederick T. Davis is the principal of Fred Davis Law Office, LLC, a Lecturer in Law at Columbia Law School, and the author of *American Criminal Justice: An Introduction.* He is a member of the Bars of New York and Paris.

No country embraced the AN0M breakthrough more enthusiastically than Australia, where it was known as Operation Ironside. Several thousand federal and local officers were involved in spreading the use of the technology and harvesting the results; when the story broke, hundreds of individuals were indicted, and their cases have been working their way through the Australian courts.

Was the AN0M Evidence Admissible Under Australian Law?

The question was complicated, depending in part on which of two laws applied to the program. Two candidates were the Telecommunications (Interception and Access) Act 1979, which requires a warrant to effect the "interception" of a communication, and the Surveillance Devices Act 2004 ("SDA"), which governs access to computer data. Acting pursuant to the SDA, the Australian police obtained warrants to permit access to the data already automatically transmitted to and downloaded by Australian authorities pursuant to their arrangements with American authorities. As the Attorney-General of Australia put it in 2024:

> Operation Ironside was a major organized crime investigation undertaken by the AFP [Australian Federal Police] between 2018 and 2021. It involved the AFP developing the capability to collect communications over the AN0M application to allow covert surveillance of alleged organized crime networks. Copies of communications sent using the AN0M application were transmitted to servers in Australia. The AFP obtained evidence from those servers in accordance with warrants independently issued under the Surveillance Devices Act 2004 and Crimes Act 1914.

A key legal question, then, was whether the AN0M program involved an "interception" in violation of the Telecommunications Act requiring a warrant permitting the original transmissions, or whether the SDA warrants authorizing access to the data already on the Australian servers were sufficient.

The Ironside Decisions

An initial ruling supported the prosecution. It reasoned that the initial transmission of data to Australian servers was not an "interception" because the data transmitted to Australia was not a "copy" of a communication between two private parties but was rather a separate transmittal – so nothing was "intercepted." Thus, under this reasoning, a post hoc warrant under the SDA granting access to this data – already downloaded in Australia – was sufficient.

Tension mounted in November 2024 when the High Court granted special leave to review this decision. Remarkably, the Parliament was so concerned about the possible outcome that it rushed through new legislation called the Surveillance Legislation (Confirmation of Application) Act 2024, which went into effect in December. It stated, with specific reference to the Ironside warrants, that the AN0M evidence was governed by the SDA and that it was not obtained by an "interception" to which any Australian law, including the Telecommunications Act, applied. As stated in the official Summary that accompanied the act, it "[c]larifies that information or a record obtained under specified warrants issued to the Australian Federal Police in connection with Operation Ironside was not intercepted while passing over a telecommunications system and was obtained lawfully under the relevant warrants." In short, the law retroactively stated that the reasoning of the court decision then under review in the High Court was now the law with respect to that case; the legislators emphasized that the act "does not change the law," going forward, and thus was intended to apply to this case only.

The arguments in the High Court focused on the separation of powers: the core question was not whether the lower court's reasoning was correct, but whether the legislative act establishing its correctness was an invasion of judicial authority. The defense argued that only the courts, and not the legislature, should interpret the laws, which, if accepted, would then have led the Court to address the procedurally subsidiary – but in fact core – issue of whether the Ironside procedures were legal. The Court rejected this argument, upheld the validity of the "for this case only" legislation, and did not provide its own analysis of whether the Ironside transmissions were "intercepted" or not. The key analysis of the court's majority was that the new act did not, per se, direct an actual outcome, but rather only established "the law" that the trial court will now apply.

> Properly construed, therefore, the impugned law in all its potential operations does not trespass on the exclusively judicial function of adjudging and punishing criminal guilt. Rather, the impugned law facilitates the admission of evidence which might otherwise be excluded by … the TIA Act… or the common law discretion to exclude illegally obtained evidence. The impugned law does not involve a "legislative judgment" of criminal guilt or civil liability.

Outsourcing?

By itself, this saga provides a fascinating insight into Australian criminal justice procedures. More broadly, it is a further anecdote reflecting the many complex interrelationships in global criminal justice initiatives. The AN0M phenomenon began as a purely American experiment, yet its most important successes were in Australia, where the local authorities appear enabled to obtain convictions based on evidence that would be inadmissible and unusable in America. Such international "outsourcing" – adopting the phrase sarcastically and critically used by a German judge to describe this phenomenon – will probably increase.