March 2015

NUJ and CIJ joint response to the interception of communications and equipment interference: draft codes of practice

The National Union of Journalists (NUJ) is the representative voice for journalists and media professionals across the UK and Ireland. The union was founded in 1907 and has 30,000 members. It represents staff and freelancers working at home and abroad in the broadcast media, newspapers, news agencies, magazines, books, public relations, communications, online media and photographers.

The Centre for Investigative Journalism (CIJ) is a charity committed to the education and training of journalists, editors and researchers towards critical in-depth reporting and defence of the public interest. The CIJ provides and facilitates the education of the public and the community in the craft, culture and methodology of journalism, for the benefit of public integrity, accountability and an informed body politic.

The NUJ and CIJ are concerned about the implications for press freedom if the UK intelligence and security agencies are permitted to access journalist's computers remotely and break encryption codes (both inside and outside the UK).

We welcomed the parliamentary intelligence and security committee report on Britain's surveillance laws and the acknowledgement that the current approach needs to change and should provide greater clarity with new legislation. We have consistently argued the existing data and surveillance rules are complex and confusing and have been laid down in numerous, badly drafted pieces of legislation, codes and guidance.

The adoption of the new surveillance powers in the draft codes enables the authorities to access computers remotely. The NUJ and CIJ believe these powers should be the subject of primary legislation and should not be introduced via secondary legislation in a code of practice under the Regulation of Investigatory Powers Act 2000 (RIPA) which itself is not limited to terrorism and serious crime but covers all crimes.

Accessing computers or other devises allows the intelligence services to obtain vast amounts of information. It would mean the authorities would have control over targeted devices and access to any information stored including encrypted data and communications. This information could include documents, emails, diaries, contacts, photographs, internet messaging chat logs, and the location records on mobile equipment. It would also mean having powers to access anything typed into a device, including login details/passwords, internet browsing histories, other materials and communications. Draft documents and deleted files could also be accessed. In addition, the microphone, webcam and GPS-based locator technology could be turned on and items stored could be altered or deleted.

If these powers are to be used, there needs to be a public debate about how this will impact on citizens as well as journalists. The powers should be introduced in primary legislation and be used only in the most compelling and narrowly-defined circumstances, with clear oversight and safeguards.

In general these powers should not be used as a fishing expedition or used to target people or devices that do not have a direct connection to a specific threat to national security or serious crime and should also be defined as having "a pressing social need". The draft code section 2.12 explicitly permits intrusion into devices that are “not intelligence targets in their own right” so long as the intrusion is treated as "intended".

Access should be subject to the highest levels of judicial authorisation and be accompanied by stringent independent oversight. Whatever body provides this oversight must have the numbers, resources and, crucially, the technical expertise to perform this function. Any individual or entity that has been targeted should be able to seek redress and these powers must not be used to circumvent other legal mechanisms for obtaining information. The strictest limitations on dissemination to outside bodies should also be put in place, not least on the transfer of information to non-UK bodies who are wholly unaccountable to the UK citizens. All data intercepted or otherwise collected should be destroyed at the end of an investigation, or in finite time, with any exemptions subject to strict tests by an independent arbiter.

The safeguards in the codes of practice proposed are not adequate to protect freedom of expression, journalists, their sources and journalism.