

---

Mass internet surveillance is 'corrosive of online privacy' – UN report

15/10/2014



*"Bulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right guaranteed by [the UN's International Covenant on Civil and Political Rights],"* UN Special Rapporteur on Counter Terrorism and Human Rights Ben Emmerson wrote in a special report to the UN General Assembly, released on Wednesday.

Emmerson's report, [published](#) in the Guardian, was a response to revelations from the world's famous whistleblower Edward Snowden on mass surveillance of users' data by the US National Security Agency (NSA) and Government Communications Headquarters (GCHQ) in the UK.

According to Emmerson, mass surveillance *"poses a serious challenge to an established norm of international law."*

*"It is incompatible with existing concepts of privacy for states to collect all communications or metadata all the time indiscriminately. The very essence of the right to the privacy of communication is that infringements must be exceptional, and justified on a case-by-case basis."*

The report adds that the use of mass internet surveillance via Prism and Tempora *"effectively does away with the right to privacy of communications on the internet altogether."*

Emmerson also mentioned one more surveillance program by the NSA – a cyber-warfare suite called QUANTUM – which *"enables secret control over servers in key locations."*



Ben Emmerson.(AFP Photo / Carl Court)

QUANTUM can *“inject unauthorized remote control software into the computers and Wi-Fi-enabled devices of those who visit the clone site,”* by impersonating websites, he added.

Emmerson said that many countries are now able to intercept and monitor the calls both from landline or mobile phones and thus can determine the individual's location. Also more and more governments use malware systems to infiltrate users' devices.

*“This amounts to a systematic interference with the right to respect for the privacy of communications, and requires a correspondingly compelling justification,”* Emmerson says.

He adds that *“merely to assert – without particularization – that mass surveillance technology can contribute to the suppression and prosecution of acts of terrorism does not provide an adequate human rights law justification for its use.”*

*“The internet is not a purely public space. It is composed of many layers of private as well as social and public realms.”*

Emmerson states that the right to privacy is not *“an absolute right.”*

*“Once an individual is under suspicion and subject to formal investigation by intelligence or law enforcement agencies, that individual may be subjected to surveillance for entirely legitimate counter-terrorism and law enforcement purposes.”*

However, he also urges states *“to revise national laws regulating modern forms of surveillance to ensure that these practices are consistent with international human rights law.”*

*“The absence of clear and up-to-date legislation creates an environment in which arbitrary interferences with the right to privacy can occur without commensurate safeguards. Explicit and*

*detailed laws are essential for ensuring legality and proportionality in this context.”*

In July, the UN High Commissioner for Human Rights Navi Pillay [told](#) reporters that the fundamentally clandestine nature of mass surveillance *“is severely hindering efforts to ensure accountability for any resulting human rights violations.”*

The commissioner warned that due to the current climate, it is increasingly difficult to even know when violations are taking place, despite the existence of *“a clear international legal framework”* which clearly sets out *“governments’ obligations to protect our right to privacy, and other related human rights.”*

---