AMNESTY INTERNATIONAL
OP-ED

AI Index: AMR 51/073/2013
25 October 2013

UN response to surveillance must strike balance between privacy and security

By Michael Bochenek, Director of Law and Policy at Amnesty International.

This week's revelation that the USA's National Security Agency (NSA) has spied on 35 world leaders has only further exacerbated international outrage about its massive electronic surveillance programme.

Besides demanding answers directly of the Obama administration, some of those targeted have taken the fight to the United Nations.

Brazil and Germany in particular are calling for a UN resolution to demand internet privacy. They are urging the international community to take action to shore up the right to privacy against such surveillance without proper oversight.

Any UN debate on the issue must not lose sight of how this surveillance is damaging to fundamental human rights. It must not be limited to protecting world leaders or cross-border surveillance. Instead, it must address – or at least start a proper discussion on – the wider impact that massive electronic surveillance programmes have on whole societies.

There's no question that the nature and extent of communications surveillance by the USA, the UK and other countries raise serious human rights concerns. The obvious one is the lack of respect for the right to privacy. Such measures also create a significant chilling effect on free expression and association.

More generally, privacy is essential to a person's liberty and dignity. It is critical to personal identity, integrity, intimacy, autonomy and communication, and has overarching benefits for society as a whole.

Any measures to interfere with privacy must always be proportionate to a legitimate aim being pursued. And justifications for doing so must be subject to judicial oversight and parliamentary scrutiny that are transparent, robust and independent.

The extent to which the USA, the UK and other governments' alleged surveillance of telephone and internet communications infringes on privacy without clearly satisfying those tests is breathtaking.

Instead of trying to show – in advance and to the public – that their surveillance

measures are necessary and proportionate, they ask their own populations and the rest of the world to trust them, blindly.

Even when individual communications are not monitored, the capacity to analyse data that have been collected in bulk and aggregated from different sources can infringe on an individual's privacy in alarming ways. It can provide a very accurate picture of a person's private life, including their associations, use of time, health conditions, political views and other details.

It's true that many of us agree to share some of this information when we use social media, apply for a loan, or change jobs. But we don't expect the bank to have access to our dating history or to know who we spend time with. In fact, laws in many countries prevent banks and employers from seeking or using some information – for example, about political views, union membership, race or ethnicity, sexual orientation, or HIV status – and for good reason.

And when we do share information with businesses, we have the opportunity to read the terms on which we're making the disclosure. But when governments are engaging in mass surveillance of internet communication, the only terms so far seem to be that it's open season; any and all intrusion on our privacy is fair game.

Put it another way – imagine a government agent sitting in your living room, thumbing through your text logs, opening up and reading through the day's emails, and making note of the websites you've visited. Would you feel uneasy about that?

And even if these governments can say that they're not giving everyone this level of scrutiny, it's still true that they can do so at any time. Some of the surveillance techniques actually allow states to collect and store the content of individual communications for years.

That might not make a difference to some of us. But in my line of work, it's a chilling thought. We know that governments routinely share the information they collect with their allies. What if part of the conversation I had yesterday with a lawyer in another country is shared with her government, which is already looking for a reason to make her stop advocating on behalf of human rights victims? Or maybe her government isn't repressive today, but what about 10 years from now?

These are serious threats to human rights. They must be met with a serious response, one that stops mass surveillance programmes from encroaching on individual liberties for the foreseeable future.

States need to take a long, hard look at the practices they're adopting and have an honest conversation about the risks they're taking. And they must commit to striking an appropriate balance between privacy and security, one that gives enough weight to the freedoms that are essential to the human spirit.