The quest for an evaluative framework for surveillance is a noble one. We all want to be guided by some framework that is widely accepted. It helps us build a language, build a community, and build something that approaches consensus on what qualifies as good or bad surveillance. But, all frameworks need to be built. They need to be accepted. This work is hard. And the work, the output, and the implementation needs to be focussed.

It is needed

We certainly need a framework for to evaluate, assess, and push back against surveillance. What Macnish is trying to do is very much needed particularly because some of the principles are lacking from other frameworks. As Marx noted previously (1998), we have the fair information principles/practices, and these are good, but are dated and do not consider modern techniques. Marx’s own 29 principles are a more reflective framework.

The beauty of Macnish’s approach is that it incorporates important principles from privacy law (proportionality), other human rights (discrimination), and accountability (authority and thereby legitimacy, and chance of success). It recognises that we should see surveillance as an exceptional act, governed under the principle of necessity.

Perhaps the most interesting contribution is that underlying everything else, there must be occasions where a particular surveillance act should not be done. Too infrequently do we have these debates, and rather we only consider when and how surveillance should be used, and we react to technological imperatives. Body-scanning was previously the line that wouldn’t be crossed; DNA preceded that; just as at one point mass fingerprinting of populations would have been considered surprising. We need to ask questions about how as a democratic people we may decide to not apply some forms of surveillance because not only are they culturally unacceptable, but because we do not wish to empower anyone with that ability to peer into our lives or treat us in such a way. My only criticism of his listing of principles is that he doesn’t spend more time discussing this most important point.

We are at a point in time where we are seeing interesting levels of discussion and debate about surveillance, particularly about relatively new forms of surveillance. Although none of this is particularly new to the readers of this journal, new public debates are emerging over ‘mass surveillance’ (previously seen in the great work of the academics in this discipline on CCTV but now being discussed in light of new capabilities to monitor vast amounts of communications), and whether it is an act of surveillance if it is merely collection with only occasional analysis (previously debated in the DNA database debates, now
being fought over metadata). We need evaluation frameworks that can help inform these debates, and act as touchstones as we try to decide what kind of rules govern how surveillance is done, or done at all.

It is hard

My concern is that by reaching for another framework, as though it is from the literature, Macnish is hoping to short circuit the hard but necessary work in building a framework. As my colleague Simon Davies always noted, process is everything. This process and consultation can’t be avoided by just pointing to the just war doctrine. In fact using just war as a touchstone may well distract from the benefit of this discussion because comparisons between war and surveillance may arise.

Instead, frameworks need to be built. And the hard work of building it through consultation and dissemination, testing and retesting, debate and redebating is what makes it strong. The strength of the fair information practices/principles is that the lineage is strong, has been debated repeatedly, in different contexts, over time and space. This does not necessarily make them good, but it makes them notable, which gives them currency in debates and deliberations.

Process may very well be the most important component to a framework. Process can’t really be controlled. We may need to allow for drift. This is what a participatory process allows as people apply their own meanings and purposes to the principles, the document, and the possible impacts.

Our experience

Within civil society we recently embarked on our own similar process to develop an evaluative framework. The ‘International Principles on the Application of Human Rights to Communications Surveillance’1 were finalised over the summer of 2013 and launched at the UN Human Rights Council in September 2013.

When we first embarked upon this initiative in the summer of 2012, I wanted them to be an evaluative framework for communications surveillance laws. At Privacy International we are working more in developing countries who were ‘updating’ their laws to capture mobile telephony and the internet. I felt that our partners in these countries were lacking a strong framework that they could use to evaluate existing and proposed laws in their countries. Meanwhile, our own work on uncovering the global trade in surveillance technologies uncovered surveillance techniques that were not foreseen by laws passed in Europe and North America in the 1990s and early 2000s. The use of trojans, IMSI catchers, and mass surveillance techniques for fibre optic cables were on the rise, thanks to Western companies selling these technologies to undemocratic and democratic governments.

We began consulting with leading experts across civil society, industry, and technologists to see if we could somehow come up with a framework to evaluate whether our current or emerging laws would match modern capabilities. In the process of discussions and drafting, we also came up with some normative decisions about what would be appropriate: the use of encryption should never be banned, intercept capabilities should not be built into new communications infrastructure, and that protections for whistleblowers were essential to deliberation about communications surveillance (even before Snowden). Other decisions were made to reflect the changes in technology policy. The most important was that we should protect communications metadata at the same level as we protect communications content.

A draft emerged, and the drift began shortly thereafter. The lawyers in our midst quickly noted that we also needed to ensure that a government’s legal safeguards not only needed to respond to modern

1 Available at https://necessaryandproportionate.net
surveillance capabilities but that human rights law needed to reflect upon these capabilities as well. And within human rights law there are frameworks and principles under the rule of law, which include asking questions about whether an interference is necessary, proportionate, and in some countries, whether due process was followed. New language was added to new drafts.

The drift continued. As more international experts became involved we found the need to expand our understanding of ‘human rights law’ to include international frameworks. Additional ‘principles’ were added, including questioning whether the laws allowing surveillance were for a ‘legitimate aim’.

Conflict and controversy was never far from the process. The attempts to bring in international human rights law also caused a rupture with the more normative decisions around protecting whistleblowing and preventing vulnerabilities. The purpose of the principles grew confusing. Some rightly saw the opportunity to enshrine international human rights law into the framework, because if done correctly, it would act as a soft-law statement on human rights which could become legally actionable in some countries. While this new purpose was tempting, it would preclude us from including the more normative components that others felt were essential to a rights-protecting system in today’s communications environment but were not necessarily recognised in international human rights law.

Debates also emerged around whether the framework should be a floor or a ceiling. Should it reflect what is reasonably achievable or what was considered necessary by some in the face of new capabilities and new risks? Should it allow for data retention, because, after all, many countries have passed laws allowing for communications data retention? Should it create a separate class of activities for intelligence agencies, because presumably having this under law was more desirable than only addressing law enforcement activities?

There are no answers to these questions. Nothing is self-evident. Rather, it is the hard work, the consultative process, and the wide-spectrum of involvement in the process that gives the results some legitimacy. There is no stone tablet with writing upon it that states that we should have specific rights. Rather, the people involved and the process that emerged created an agreed text against which we can aspire, evaluate, and judge.

As there are no answers, there is never a strong settlement. Just as international treaties, laws and other texts can be ignored or modified, these principles will likely change. In some areas there are still disagreements. For instance, our requirement that governments must notify individuals of the decision authorising communications surveillance with sufficient time to appeal is controversial for some, while others see it as necessary. I’m of both opinions. Secret surveillance was, at least under the rule of law, a rarity when governments had to show a warrant to come into your home. If they wanted access to files you had on your computer, again secret surveillance would normally have been a rare event. Today, governments can perform surveillance without asking you but rather need only issue an order against a service provider, or through compromising your devices. If all your files, biographical, medical and financial were to be made available you would think that you have the right to object. But it is also true that governments sometimes need to do this surveillance in secret because it may compromise their investigations to notify you. Interestingly, few disagree that government should eventually notify the individual of the surveillance, as some laws already require but is rarely done.

The principles have been signed on to by over 400 civil society groups, with tens of thousands of individuals who have also signed on to date. Will they be accepted as the standard for evaluating communications surveillance laws? In a sense, only time will tell if they become something close to ‘soft law’. Nonetheless, we have over 400 civil society groups from across the world who now have access to this evaluative framework and may use it to feed into national and international deliberative processes. And even more importantly, the process of deliberation and debate informed people even more so about
the issues surrounding communications surveillance. Even if the principles are never referenced or used again, the hard work was invaluable to those who participated.

Concluding thoughts

It is a rare event when someone steps up with draft text and states that these will be the principles to which we will bind future human activity. This is indeed fortunate, because no single individual or document can achieve this without buy-in. We are even more fortunate because no single individual or document is endowed with the necessary wisdom with which we would like to bind future human activity. This is why we need a good process. Adopting a ‘just surveillance’ approach isn’t problematic per se, and embarking on this by saying that this is a good starting ground isn’t a bad idea, but we must allow for drift and development, and hope the results are promising.

References