In the interest of time, I will focus on only one of the guiding questions, regarding examples that best illustrate the relationship between technical standards for new and emerging digital technologies and human rights. One example is the adoption of Dual EC DRBG which was recommended by the NSA to NIST. Werthheimer, the Director of Research at NSA, wrote in a letter that, "With hindsight, NSA should have ceased supporting the Dual_EC_DRBG algorithm immediately after security researchers discovered the potential for a trapdoor.

In truth, I can think of no better way to describe our failure to drop support for the Dual_EC_DRBG algorithm as anything other than regrettable." Indeed, this was a gross violation of public trust, since many companies and people were misled by the NIST which gave its seal of approval and safety to a faulty random number generation algorithm. Michael M. Kelsey, a cryptographer at NIST realized this discrepancy and possibility of a backdoor.

This is why technical standards must be source-neutral. The NIST put too much trust in the NSA and completely failed its guarantee to provide cryptographically safe algorithms. Who knows what could have been done with the trapdoor. Perhaps the vulnerability was exploited in unethical ways that put the lives of other people at risk.

I conclude by citing one of the most important philosophers in the history of western philosophy: Kant. In his *Groundwork to the Metaphysics of Morals*, he postulates, "So act that you use humanity, whether in your own person or in the person of any other, always at the same time as an end, never merely as a means" (4:429). Clearly, cryptography challenges us to make ourselves accountable to this supreme practical principle, that is, the second formulation of the categorical imperative, the famous formula of humanity. That is why technical standards will always have a crucial relationship with human rights, for in order to treat humans as ends instead of means (and respect the dignity of every individual), the cryptographic community must ensure that it is not blinded by the prestige or political motives of any organization. It must conduct its technical standards in a rigorous, neutral, and well-balanced manner.