ECON 425/563 // CPSC 455/555

This is the second part of HW5. It is due on Tuesday, December 2, 2008, together with the first part.

3. **Copyright enforcement vs. privacy protection**. At first glance, copyright enforcement and privacy protection seem to be similar problems from a technical perspective. In particular, major players in the computer industry [TCG] have made the argument that both problems can be solved by widespread adoption of *trusted systems*. Roughly speaking, a trusted system is a hardware and software platform that can prove that it is running approved software. That is, if A and B are "trusted" computers connected by a network, and the owner of A wants to transfer some sensitive data to the owner of B, then A and B can execute a protocol during which B proves to A that it is running the operating system and application software that A requires for the processing of these data. Modern PCs ship with trust platform module (TPM) chips that could play an important role in the construction of such systems.

The potential applicability of such systems to copyright enforcement is clear: Entertainment-content distributors could insist that client machines prove that they are running approved, DRM-enabled player applications before the content is downloaded. Note that the proofs (or "attestations") in this scenario would be done by end users' machines, and the rules that they would have to prove that they are complying with would be determined by copyright owners, which are often large corporations. What is unclear is why users would buy these systems, since they are in some ways less capable than ordinary ("untrusted") PCs.

One answer that's been offered is that privacy protection is analogous to copyright enforcement but that, in the privacy scenario, it's the end user that enforces the rules. If a user is considering transferring his personal data to a server, he can insist that the server first prove that it is running a system that is appropriately privacy-sensitive (e.g., a HIPAA-compliant system [HIPAA] in the case of health data).

Give three reasons that this analogy is flawed, and briefly explain each one.

[HIPAA] Health Information Portability and Accountability Act, http://www.hhs.gov/ocr/privacysummary.pdf

[TCG] Trusted Computing Group, https://www.trustedcomputinggroup.org/home