There are 4 things in my hand: tool for understanding technical measures

All 4 have owners, all 4 can have “technical measures” applied to them

1) Medium: CD's, DVD's, sometimes nothing (downloads)

2) Content: music, movies, text,software, ...

3) Hardware: CD/DVD players, TV, phones, computers, cameras, ...

4) Software

- Content is passive, and can not make decisions on its own
- Content can be manipulated in various ways to accomplish various goals
- Cryptography: convert ordinary content (plaintext) to gibberish (cyphertext). Used for confidentiality, integrity, authentication, signatures
- Watermarking: embed information in other data. May be visible/invisible, used to identify data, confidential message
- At the other end of a “download” is a (hopefully) secured computer/network

- Hardware simply follows instructions in the form of software, and is where any “decisions” or other activity happens
- Computer security is all about ensuring that only authorized software runs, or that only authorized persons are able to run software
- Authentication: Something you have (ID card, key), something you know (password), something you are (biometrics)
- Data stored within hardware (disk drives, flash memory) can be secured as with any other content

Key Question: Who owns what is locked, and who has the keys?