Public sector must follow laws. Fourth amendment, case law, etc. Department of justice maintains a reference. Computer fraud and abuse act of 1986 and state laws.

4th amendment: to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated, and no warrants shall issue but upon probable cause supported by oath or affirmation describing the place to be searched and persons or things to be seized.

There are some specific exceptions: if the expectation of privacy is not one society deems reasonable.

Computers are to be treated as closed containers. Usually a warrant is required.

Communications in transit are private. Upon delivery they are now free reign, and a third person expectation of privacy does not exist. The recipient can report or do whatever they want with messages.

Private sector has much more flexibility in investigating. Must follow policy. Policy violations, litigation disputes, email harassment, falsification of data, discrimination, embezzlement, sabotage, industrial espionage.

Pen testing pays well. Zero day attacks when a fresh patch or version comes out.

Terms of use/ internal warning banners provide warnings and limitations to use.

Same with an acceptable use policy basically.

Line of Authority: states who has the legal right to initiate an investigation, take possession of evidence, and who can have access to it.