And we go through use share and archive eventually we get to a point in time where the data is going to be deemed, to be ready, to be destroyed. Meaning it either no longer has value in our organization or the useful life of that data has been exceeded, or the value is no longer relevant or any reasons why we want to destroy data. It's a slow Monday we've got nothing going on right we may need a hobby but we don't have one whatever the case may be. W e'regoing to destroy data so Daniel when we go to destroy data what in your mind, what would you think of. A saying would be essentially a good way to destroy that right in other words a secure way away. That's risk-adverse a way that would align with our data management policies what would come into your mind what would you think typically. I've seen them used like giant shredding machines where we take the actual physical disk if the data relies on our lies on and then we put it through some sort of destruction mechanism and it physically destroys. The disk so that cannot be recreated that's probably one of the best ways I can think of to actually get rid of that in other ways it's like scrubbing the data off of the disk if you're going to reallocate that actual space, and using like the government level where rights ones and zeros in the erases. It rights one of the kids multiple overrides write multiple overrides ok so multiple over Xbe good way big fancy shredding machines another good way to do it. Basically you know we may have a menu of options right is my point of what Danielis describing this essentially several different ways or at least two of them anyway we may go through and do other things. We may actually physically not just shred the drive but liquefy it essentially throw it in a gas furnace or somethings trap a block of thermite through it. You know whatever you may do right but we'll essentially destroy any physical particulate matter associated with the drive render it inoperable in some way we may decide to go in and we may decide to cryptographically erase the data. As you said multiple overwrites we may degauss the drives use a strong magnetic field to either wipe the drive or at least rearrange the particles in such way that can't be retrieved. But everyone of these options short of actual physical destruction and even something like a shredding machine depending on how thorough the shredding is may leave behind matters sentially bits of the magnetic platters. If it is a normal magnetic drive or if it is an SSD drive may leave behind bits of storage mechanism the flash memory essentially that not by the average person and probably not by the average company. But by certain entities typically government entities and entities at work for governments that have letters in their name that are typically acronyms right. They may be able to go in and recover some data from those random bits but the average individual the average business the average company is probably<not going to be able to do much with that pile of garbage so the question really becomes what level of assurance right are we looking for with regards to data destruction.