According to the textbook, there are 34 key laws in the United States which possess a significant influence on the InfoSec community. The Federal Trade Commission Act of 1914, FCRA of 1970, FERPA of 1974, HIPAA of 1996, COPPA of 1998, CAN-SPAM Act of 2003, American Recovery and Reinvestment Act of 2009, and HITECH Act of 2009 serve to protect the consumer from deceptive advertising practices, misuse of private information, and breaches of personal health information. The Federal Privacy Act of 1974, Electronic Communications Privacy Act of 1986, Exception 18 USC 3121 et seq., USA PATRIOT ISA of 2006, and USA FREEDOM Act of 2015 cover how the federal government can initiate wiretaps, what communications they are permitted to eavesdrop on, and the government's usage of private data. The 18 USC 2701 of 1986, CFA of 1986, National Information Infrastructure Protection Act of 1996, No Electronic Theft Act of 1997, DMCA of 1998, Identity Theft and Assumption Deterrence Act of 1998, 18 USC 1029 of 2004, and ITAR Act of 2012 all serve to criminalize illegal behavior conducted digitally like identity theft and software piracy. The CSA of 1987, the creation of Part 11 in Title 21 in 1997, the FISMA of 2002, the National Cybersecurity Protection Act of 2014, the Federal Information Security Modernization Act of 2014, and the Cybersecurity Workforce Assessment Act of 2014 ensure that the federal government is employing the proper cybersecurity measures to protect the information they hold and the infrastructure they control.

When only considering the impact detailed by the book, I feel that the majority of the laws listed above are appropriate and necessary. In my opinion, we need more laws criminalizing certain digital behavior and more laws to protect consumer rights, especially privacy. Laws like GDPR are an excellent move in the right direction but even that isn't powerful enough. The laws forcing the executive branch of the federal government to enforce proper security is extremely important due to the rise in cyberwarfare and cyberterrorism that could cripple the United States or its infrastucture. However, I do not support all of the laws which govern wiretapping as I believe that laws like the USA FREEDOM Act and the USA PATRIOT Act grant the government should be restricted to protect people's privacy. While there does need to be laws dictating the extension of search and seizure into the digital realm, those particular acts provide too much power and are poorly thought-out, knee-jerk responses to tragedies like 9/11. There are other laws listed by the book that I did not include in one of the lists above. Some of them, like the SAFE Act, are definitely relevant to cybersecurity and are extremely important but didn't fit into the broad categories outlined above. For others like the FOIA or the EEA, I struggle to see their relevance to cybersecurity or why they were included in the list. However, that does not diminish their importance in other fields where I lack the knowledge to determine their appropriateness.