Legal Evaluation of Interception Capabilities The government has put in place stringent controls on interception of electronic communication with an objective of ensuring privacy of users.Even for internal network security, monitoring must be limited to protecting AD's own machines, and the BYOD WiFi policy (limiting to external access only) suggests employee computers are not wholly under AD's control, potentially requiring explicit user consent to avoid Wiretap Act problems. 2701 et seq.) that regulates unlawful access to stored emails and data and the Pen Register and Trap and Trace Act that directs the collection of signaling and routing information.Government partnerships can facilitate threat intelligence sharing with the Cybersecurity Information Sharing Act (CISA, 2015), but CISA allows voluntary sharing, not active intercept (Congressional Research S., ervicen.d.).2511) criminalizes deliberate interception of electronic communications in transit without consent or a court order, the Stored Communications Act (SCA) (18 U.S.C. ?Also important in this case study is the Cybersecurity Information Sharing Act (CISA, 2015) regulates the voluntary sharing of threat indicators between companies and government agencies but prohibits interception without proper consent or warrant.Additionally, the company should enhance minimization in the sense that if interception occurs under consent they should collect only the required information and ensure minimal retention.To achieve this, crucial statutes have been passed into law and these include the Electronic Communications Privacy Act (ECPA, 1986) under which other subcategories exist such as; Wiretap Act (18 U.S.C. ?This is because, the company utilizes OC circuits owned by and operated by Google Fiber, a third-party service provider. 1030) that prohibits unauthorized access and CALEA (Communications Assistance for Law Enforcement Act, 47 U.S.C. ?Interception is prohibited under the Wiretap Act except where it meets certain exceptions, such as where consent is given by one or more parties (18 U.S.C. ?And since AD is not a telecom provider, it cannot rely on carrier authorities that might allow widespread interception.To mitigate this legal litigations, the company should ensure a written, informed consent for devices whose traffic may be intercepted.Moreover, interception requires consent or legal authorization.Moreover, court orders that warrant interception must be sought especially when coordinating with government officials.1001) that is entirely applied among telecom provider are stated.As such, a party of the communication must consent and this should be explicit and well documented.Moreover, AD government contracts do not by default include interception rights.Indeed, BYOD users must sign explicit terms.From a legal standpoint, AD is not legal enough to warrant interception.2511(2)(d)) or activity by a communications service provider in defense of its rights or property (18 U.S.C. ?For traceback against outside attackers, AD would need a court order under 18 U.S.C. ?CFAA (Computer Fraud and Abuse Act, 18 U.S.C. ?2518 with probable cause and judicial warrant for up to 30 days.2511(2)(a)(i)).