ENTRUST

SECURING A WORLD IN MOTION

Entrust's Response to Government Requests for Customer Data

The court in *Schrems II* was principally concerned with the ability of US law enforcement to reach EU personal data through mechanisms such as Foreign Intelligence Surveillance Act (FISA) Section 702 and other intelligence gathering activities under Executive Order (EO) 12333, or "no notification" orders under the Electronic Communications Privacy Act (ECPA), authorized by a court, which allow for records requests to electronic communications service providers and generally do not permit immediate notification to the data subject of the existence of the order. The US Department of Commerce published its formal response to the decision in September 2020 to specifically address questions and concerns about the use of these mechanisms to reach personal data. We encourage customers to read this white paper.

Entrust is unlikely to receive such a request for customer personal data under FISA 702, EO 12333, or the ECPA. However, this document outlines the steps Entrust will follow in the event we receive such a request.

» **We will notify an affected customer of any legally binding and valid request for its data or any direct access to customer data by a law enforcement or other government agency unless we are explicitly prohibited from doing so by law.**

» **Where possible, we will refer the requesting government agency to the affected customer.** Entrust is not the owner of our customers' data, and it is our position that any government agency seeking access to customer data should address its request directly with that customer, where possible.

» **We do not disclose customer data to government agencies unless compelled by law and we will challenge unlawful requests.** We will review each government request for customer data and will only comply if and to the extent we determine the request is legally binding and valid. We will require government agencies to follow the required legal process under applicable laws, such as issuing their request via a subpoena, court order, or search warrant. We will attempt to challenge government requests for customer data when we believe them to be invalid or unlawful.

» **If we are required to disclose customer data to government agencies, we will ensure the transfer is necessary and proportionate and provides the minimum amount of information possible while still complying with the order, based on a reasonable interpretation of the government request.**

» **If prohibited by law from notifying the affected customer, we will try to get that legal restriction waived.** If we receive a government request for data, and we are prohibited by law from notifying the affected customer, we will request the confidentiality requirement be waived to enable Entrust to notify the appropriate data protection authorities.