

## AWS och CLOUD Act

av Michael Punke |

Samtidigt som nyheter om Brexit dominerar tidningsrubrikerna i Storbritannien, inträffade en annan viktig händelse i London nyligen. USA:s biträdande statsåklagare, Richard W Downing, gick igenom fakta och myter bakom Clarifying Lawful Overseas Use of Data Act (CLOUD Act), i ett [tal](#) vid Academy of European Law Conference (ERA). Efter talet publicerade US Department of Justice (DOJ) en [vitbok](#) och en [FAQ](#) som klargör syftet med, och omfattningen av, CLOUD Act och reder ut många av de missuppfattningar som denna lag har gett upphov till.

Jag uppmanar alla som är intresserade av CLOUD Act att läsa talet, DOJ:s vitbok samt FAQ:n för att få bättre förståelse för vad CLOUD Act faktiskt innebär - och vad den inte innebär. Enkelt uttryckt innebär CLOUD Act ett antal mindre uppdateringar av en flera årtionden gammal lag, som begränsas till att hjälpa brottsbekämpande organ bekämpa och förebygga risken för internationell brottslighet och terrorism. Detta ger INTE, som olika aktörer påstår, amerikanska brottsbekämpande myndigheter fri tillgång till data lagrade i molnet.

Vi ser justitiedepartementets vägledning som ett steg i rätt riktning, men mer behöver göras av ansvariga myndigheter runt om i världen för att utbilda kunder inom offentlig sektor om viktiga frågor kring datalagring och datainnehav. Därför vill jag lyfta fram några av de vanligaste missuppfattningarna som rör CLOUD Act-lagen, för att våra kunder ska kunna känna sig trygga i att lagen inte påverkar hur de använder molntjänster.

### Hur lagstiftningarna haft tillgång till uppgifter under de senaste 30 åren

1986 antog USA:s kongress Stored Communications Act ("SCA"), en lag som behandlade rättsvårdande myndigheters rätt att få tillgång till elektronisk kommunikation. Även om SCA betraktades som framåtblickande när den antogs har domstolarna under många år brottats med att tillämpa lagtexten på modern teknik, som appar och molntjänster - företeelser som inte existerade när SCA godkändes. Ett av diskussionsämnena har varit om USA:s brottsbekämpande organ skulle få tillgång till data som ligger lagrade i datacenter utanför USA. CLOUD Act skapades för att sätta punkt för den diskussionen.

Den tydliggör att leverantörer som omfattas av amerikansk lagstiftning, till exempel ett företag som bedriver affärer i USA (inklusive utländska koncerner med amerikanska dotterbolag) kan få ett domstolsbeslut enligt SCA-lagen, som innebär att de måste lämna ut uppgifter som de har kontroll över, oavsett var den informationen är lagrad.

Här är det viktigt med tydlighet. Trots att många påstår motsatsen så introducerar inte CLOUD Act något nytt koncept. Regeringar över hela världen har länge haft möjlighet att kräva bevis på brott, även om bevismaterialet ligger utanför deras egna landsgränser. Som DOJ påtalar i sitt white paper kräver de flesta länder att data överlämnas oavsett var den lagras. Detta är också i överensstämmelse med Budapestkonventionen, som var den första internationella konventionen som syftade till att förbättra samarbete och utredningar kring cyber- och datorbrott. Exempelvis har franska domstolar sedan länge tillåtit landets polis att begära in data utanför Frankrike så länge det är tillgängligt från en dator i Frankrike. I februari 2019 antog Storbritannien en lag som ger de brottsbekämpande myndigheterna i landet tillstånd att begära lagrad elektronisk data från ett företag eller en person som befinner sig utanför Storbritannien.

Denna praxis bygger på en sekelgammal princip om internationellt samarbete. Länder använder olika legala verktyg, allt från inhemsk lagstiftning till internationella fördrag, för att få tillgång till potentiella bevis som utanför landets gränser, Samarbete över gränserna är en tradition som upprätthålls och en grundförutsättning för att väl ansedda organisationer som exempelvis Europol har kunnat utföra sitt arbete. CLOUD Act speglar helt enkelt vad dessa brottsbekämpande organ och länder redan har gjort i många år.

### **Att förstå CLOUD Act**

Ett av de vanligaste missförstånden om CLOUD Act är att lagen endast berör amerikanska företag. Detta stämmer inte. CLOUD Act gäller samtliga kommunikationstjänsteleverantörer eller molntjänsteleverantörer som lyder under amerikansk jurisdiktion, inklusive e-postleverantörer, telekomföretag, sociala medie- och molntjänsteleverantörer, oavsett om deras huvudkontor ligger i USA eller i ett annat land. Detta innebär att alla utländska företag med kontor eller dotterbolag i USA omfattas av CLOUD Act. Även webbplatser utanför USA, som har använts av amerikanska kunder, ligger enligt domstolsbeslut inom amerikansk jurisdiktion och kan därmed omfattas av CLOUD Act.

Ett annat vanligt missförstånd om CLOUD Act är att detta ger USA:s regering obegränsad tillgång till data som innehas av molnleverantörer. Detta är helt enkelt fel.

CLOUD Act ger inte brottsbekämpande organ fri tillgång till data lagrade i molnet. Lagstiftare kan enbart tvinga tjänsteleverantörer att tillhandahålla data om de uppfyller de mycket stränga kriterierna för en fullmakt som utfärdats av en amerikansk domstol. Amerikanska domstolar ställer mycket höga krav för att utfärda en fullmakt. Bland annat krävs det att en oberoende domare bedömer att den brottsbekämpande instansen har rimliga skäl att begära ut informationen, att informationen är direkt relaterad till ett brott och att begäran är tydlig, precis och rimlig. Detta är raka motsatsen till obegränsad tillgång.

När Amazon Web Services tar emot en begäran om data som ligger utanför USAs gränser har vi olika verktyg för att bestrida den och lång erfarenhet av att göra just det. Faktum är att bestridandet påbörjas långt innan ett ärende går till domstol. Varje förfrågan från en brottsbekämpande myndighet granskas av ett team av jurister. Som en del av granskningen bedömer vi huruvida begäran bryter mot lagarna i USA eller i det främmande land där uppgifterna finns, eller om den skulle kunna bryta mot kundens rättigheter enligt gällande lagar. Vi tillämpar noggrant gällande rättsliga normer för att begränsa - eller direkt avvisa – en eventuell begäran om data som kommer från en nationalstat, inklusive USA. Vi skickar regelmässigt dessa förfrågningar där vi uttrycker vår legala ståndpunkt, och detta resulterar ofta i att begäran om information återkallas.

Om vi inte kan lösa en tvist som uppstått mellan oss och en myndighet som begär ut information, tvekar vi inte att gå till domstol för att hävda vår kunds rätt. Amazon har en lång historik av att formellt utmana regeringars förfrågningar om kundinformation som vi anser är överdrivna eller på annat sätt olämpliga. Vi kommer att fortsätta att ta strid kring förfrågningar som vi anser strider mot lokala lagar, som [GDPR](#) inom EU, och göra allt vi kan för att skydda kunddata.

Vi kommer även fortsättningsvis att meddela kunder innan vi lämnar ut data och vi tillhandahåller avancerade krypteringstjänster som kunder kan använda för att skydda sin data ytterligare. Vi har branschledande [krypteringstjänster](#) som ger våra kunder ett flertal alternativ för att kryptera data på väg till- och från molnet – och i vila – och möjligheter att hantera krypteringsnycklarna på ett säkert sätt. Krypterad data är helt värdelös utan tillhörande krypteringsnycklar.

## **CLOUD Act har inte förändrat molnleverantörers förmåga att skydda sina kunder**

Amazon Web Services värnar om kundernas integritet och säkerhet. Vi har åtagit oss att tillhandahålla alla kunder – inklusive många myndigheter som anförtror oss att lagra data med mycket högt skyddsvärde – marknadens mest omfattande svit av säkerhetstjänster och funktioner, för att säkerställa fullständig kontroll över deras data. CLOUD Act har inte ändrat eller försvagat detta åtagande.

Tvärtom erkänner CLOUD-lagen rätten för molnleverantörer att utmana förfrågningar som strider mot ett annat lands lagar eller nationella intressen och kräver att regeringarna respekterar lokala rättsregler. De myndigheter som känner oro över huruvida CLOUD Act påverkar deras möjligheter att behålla kontrollen över sin data behöver inte göra det. Amerikansk lagstiftning innebär ett mycket starkt skydd för utländska myndigheter, när informationen omfattas av principerna för nationell suveränitet. De kan därför själva förhindra utlämning av data.

## **Kunder runt om i världen kan fortsätta att använda AWS utifrån lokala lagar och regler**

På AWS hjälper vi ständigt kunder och partners att förstå sina rättigheter i förhållande till nya standarder, lagar och regelefterlevnad. Vi tror att det är det bästa sättet för organisationer att skydda sina slutanvändare. När du har läst Downings tal och dokumenten från DOJ rekommenderar jag att du besöker vår [hemsida](#) dedikerad till CLOUD Act, som innehåller svar på vanliga frågor, en vitbok och andra resurser för kunder och APN-partners. På den webbsidan kan du lära dig mer om CLOUD Acts begränsningar och förstå hur AWS påverkas av lagen.

Man får inte heller glömma att molntjänster spelar en mycket viktig roll i samhället, inom alla möjliga områden. Med AWS molntjänster skapar våra kunder innovationer som formar hur vi lever, hur vi delar med oss av bilder eller video, hur vi shoppar och gör bankärenden, hur vi fortbildar oss och utvecklar vår kompetens. De skapar AI- och maskinlärningsbaserade lösningar för att öka industriföretags konkurrenskraft. De skapar samhällsnytta genom exempelvis bättre service till medborgare, mer effektiv brottsbekämpning, och medicinsk forskning.

Det skulle vara en mycket allvarlig och sorglig utveckling om denna innovation skulle sakta ned på grund av ett grundläggande missförstånd om hur CLOUD Act-lagen fungerar. Den information som nyligen lämnats av DOJ angående CLOUD Act utgör ett steg mot ökad förståelse, och vi hoppas att det här inlägget och relaterade resurser kommer att ge ytterligare insikt och klarhet i debatten.

Michael Punke är Vice President Public Policy på AWS