老师、各位同学好。

我们组今天主要讨论关于云平台跨境数据治理这个问题的研究和思考。

那为了方便大家理解这个问题呢，我们可以先设想一下这个场景：企业把订单存在国内云平台，请境外服务商分析销售，原来只允许发送地区、订单和销售额，系统更新后却把手机号也发了出去。

那么怎么在发出去之前发现并拦住多传的数据？那这就是我们接下来要讨论的问题。

（翻页）

那这个是我们的汇报顺序，我会先从背景开始讲起，为什么需要跨境传数据，有哪些风险，然后是现行规则和实际案例，最后是我们提出的方案。

（翻页）

那么首先是关于这个问题的背景。

（翻页）

如我开头提到的背景所述，这是一个很常见的场景。那么其他的场景还比如说跨境物流，可能有收件人信息，以及再比如说医学研究，有健康和遗传数据。

那么最关键的是，比如把账号和浏览记录关联起来，就会更容易识别某个人的行为，那这就是关键的风险所在，数据组合后，原来的风险判断也需要重新检查。

（翻页）

不过呢，还是需要强调一下，就是说这个跨境协作确实还是必要的，那具体场景具体分析，销售分析可能只需要地区和销售额，物流配送才需要收件信息。每多传一项，都要说清它对当前任务有什么必要作用。

（翻页）

那么在实际的数据传输过程中，我们就要明确整个儿的这个跨境业务链路。

那么在图中可以看到，你看首先是业务系统，然后数据存进境内云，经过出口网关，交给境外接收方。那么在这个过程中无论是向外发送还是境外人员远程查询，他就得纳入检查，对吧，企业定用途，平台控出口，接收方按约使用。

（翻页）

那么那么在这样的一个背景之下呢，我们其实也已经有了较为完善的现存数据出境规定、合同和评估制度，这种。

（翻页）

那比如说，以中国为例，现在呢我们其实是有这样的一个出境程序三层安排，那么就区分了豁免、标准合同或认证、安全评估。豁免手续也仍有保护义务。

包括欧盟的标准合同条款这种，对吧，也是传输机制，重点就在于这个规则呢它是主要判断了数据性质、涉及人数、业务目的，还有参与方身份和保护能力这样的四个部分。

（翻页）

那么在这样的现存制度下呢，现在我们实际上是会按照图中所示的这样从收集到境外使用这种链路来管理。

大致分为五个部分昂，举个例子，比如说销售数据，那你按照图里的路径来看，它是不是就会从收集到出境准备，然后发送、境外使用和后续监督，然后一看，诶，这里多了一家合同没写的接收方，那是不是就会需要核查这次传输是否获准，这样子？

（翻页）

那接下来我们看一些特别突出的几个典型的实际的例子，我们就会发现问题了：

（翻页）

那你看比如说，这个产前检测案例，他当时涉及诊所、合作方和实验室，那么就出现了一个责任和数据去向说明不清楚、不一致这种问题；

再比如说最近这个比较火爆的deepseek，对吧，他当时就把用户输入传给了火山引擎。那你看关键是他说“使用火山引擎的云服务，是为了修复安全漏洞、改善用户界面和用户体验”，但韩国监管认为传输用户输入并无必要。对吧这些都反映了，约定和说明需要与实际传输核对，这样子，对吧。

（翻页）

那这个问题的本质其实就是：一个原本获准的传输安排，那他在系统更新的时候，是不是就可能多传数据？这个问题我们就称之为“动态授权失配：业务运行过程中，实际数据传输的内容、接收方、用途或路径与既有授权条件不一致的状态”，那本质上就是现在传的超出了原来允许的范围。

（翻页）

那在这样的问题背景下呢，我们就提出持续检查、按规则执行的方案。

（翻页）

我们期望构建这样的一种机制和数据链路：就是在常规的，正常的主体业务中，我们就还是按负责人确认的规则，由出口网关检查并放行数据。

但是同时呢我们维护一个持续在线的agent bot，在整个跨境主体业务的工作过程中，我们这个bot会定期或者在配置变化后，对照审批、设置和日志。

它主要是在做找差异、报给负责人复核这样一个检查，不能自行扩大授权。网关每次执行规则，也不用等它临时判断。

（翻页）

那比如说多传手机号这种问题，以此为例，在这种接口更新的情况下，他会先查出新增字段，再与审批记录比较，发现没有获准，就报告负责人。

每次发送时，网关还会独立核对允许清单。只要能读出数据，并规定清单外字段不准发送，就能拦住手机号。负责人再决定删除字段，或者审查后更新规则，记录当时的处理依据。

那这样的话就可以拦住额外传输，就可以让系统更新后的发送持续受到审批条件约束。

（翻页）

那这种检查与执行的分工，其实已经有亚马逊的敏感数据识别服务、OPA和Envoy很好的组件支持，也在逐渐成为我们把方案具体化的基础，所以有实际实现的路径。

当然我们也认为仍有一些需要进一步细化深化、具体问题具体分析的细节需要考究，比如误拦和延迟，或者说绕过网关的路径、境外实际用途，那这也是希望我们，以及做业务、技术和合规的同学来一起验证和完善，希望可以形成经得起实际测试的方案。

（翻页）

那么我们以上从背景、规则、案例到方案这些方向讲了跨境数据的持续治理，希望可以和大家一起把允许范围与实际传输对应得更清楚。

（翻页）

那这一页是我们研究过程中主要参考的一些文献和资料等。

（翻回到thanks页）

那，感谢老师和各位同学聆听，请老师指正。