ICANN69 | 虚拟年度大会 — GDPR 下的 WHOIS 变革：对最终用户和公共安全的影响
中欧夏季时间 2020 年 10 月 21 日星期三 10:30 至 12:00

[本次会议正在录音]

欧赞 • 萨辛 (OZAN SAHIN)： 谢谢大家！欢迎大家参加“GDPR 下的 WHOIS 变革：对最终用户和公共安全的影响”全体会议。我叫欧赞 • 萨辛，是本次会议的远程参会经理。请注意，本次会议正在录制中，并遵循 ICANN 的预期行为标准。

在本次会议期间，只有在提问窗格中用英语提交的问题或意见才会被大声读出来。该功能可以从 Zoom 工具栏访问。我会在本次会议的主持人指定的时间大声读出这些问题和意见。

本次会议提供实时速记和口译服务。若要查看实时速记，请点击 Zoom 工具栏中的的“隐藏字幕”(Closed Caption) 图标。本次会议提供阿拉伯语、中文、英语、法语、俄语和西班牙语的同声传译服务，该服务将使用 Zoom 和由 Congress Rental Network 运营的远程同声传译平台同时进行。建议与会者按照 Zoom 聊天室中的说明或从会议网页上提供的会议详情文档中下载 Congress Rental Network 应用。

如果想发言，请在 Zoom 会议室里举手，待会议主持人叫到名字后，我们的技术支持团队将允许你取消静音。为了方便记

*注：本文是一份由音频文件转录而成的 **Word**/文本文档。虽然转录内容大部分准确无误，但有时可能因无法听清段落内容或纠正语法错误而导致转录不完整或不准确。本文档旨在帮助理解原始音频文件，不应视为权威性的会议记录。*

录，请说出你的姓名，如果你使用英语以外的其他语言，还要说明你要使用的语言。

发言时，请务必将所有其他设备静音，包括 Congress Rental Network 应用程序。同时，请大家发言时口齿清晰并保持正常语速，以便口译人员能准确翻译。

强调一点，在本次会议期间，如果没有技术支持团队的帮助，远程参与者将无法点击麦克风按钮自行取消静音。

所有参加本次会议的与会者都可以在聊天窗口中留言。方法是，使用聊天窗口中的下拉菜单，选择“回复所有讨论组成员和与会者”，这样所有人都能看到你输入的内容了。

注意，Zoom 网络研讨会仅支持专家讨论组成员之间的私聊。因此，专家讨论组成员或普通与会者向另一位普通与会者发送的任何消息都对其他所有主持人、联合主持人和专家讨论组成员可见。

接下来，我会把时间交给乔纳森 • 扎克 (Jonathan Zuck)。

乔纳森 • 扎克： 谢谢。我是一般会员咨询委员会的副主席乔纳森 • 扎克。你们中的很多人都知道，今年，DNS 滥用和其他相关问题可以说是成为了一般会员社群的一项主要议题，但我觉得，很多这类讨论都是重复的，没有具体到任何特定的点上。而且很多都是缺

乏数据所致。各方都有很多托词，这使得对这些话题进行理性的讨论变得非常困难。

在 ICANN 的背景下，我们经常会看到这种情况，那就是，有时候，人们在对新政策热情高涨时做出的预测并不会实现，而是会导致一些其他的结果发生。例如，最初提议新 gTLD 项目时，Sony 在一次资格听证会上称，他们将投资 1,200 万美元用于防御注册，但最终他们没有这么做。他们找到了另一种方法，来实现在这些新 gTLD 中对其商标的保护。

GDPR 的执行及随后 ICANN 社群给我们敲响的警钟与之类似，当时出现了混乱，对吧？那导致我们实施了临时规范，并且组建了一个快速 PDP 工作组负责研究 ICANN 如何才能符合 GDPR 规定。结果，可通过 WHOIS 系统公开获取的数据发生了巨大的变化，一种新的系统被建立起来，在这个系统中，人们必须向签约方提交信息请求才能获得数据。

所以在整个 EPDP 流程中，不管是好是坏，都出现了数据管理方和数据请求方，他们成为了这些讨论中的两大重要方。

本次全体会议的目的是将这两方聚集到一起，讨论在这个过渡时期究竟发生了什么。换句话说，人们提出了什么级别的数据请求，以及这些请求是如何得到处理的。我们似乎经常惊讶于实际数字比我们想象的要小，实际并没有那么多请求，或者没有那么多有关合同合规的投诉等等。所以，当我们试图就注册人数据及其使用展开对话时，以事实为基线感觉会更好。

很有可能的是，最关心注册人数据获取的各方已经找到其他途径来获取进行商标维权、开展执法活动和保护消费者所需的这些信息。所以我们现在要做的就是弄清楚我们目前的状况，以及几年后我们将处于什么状况，包括数据方面，对数据的需求，数据的可用性，以及数据请求方从签约方那里得到这些数据的效率等等。这就是我们希望在这次全体会议上展开的对话，简单来说就是一次实况调查，看看现在的情况是什么。

希望我们能尽量少做一些意识形态的讨论，尽可能地讨论有关现状的数据和事实。

正式开始讨论之前，我们先来了解一些数据请求方的看法，包括执法机构和消费者保护机构。所以在接下来的十分钟里，将由 FTC 的劳伦 • 卡宾 (Laureen Kapin) 还有加布里埃尔 • 安德鲁斯 (Gabriel Andrews) 从执法机构的角度，谈谈对这些数据的需求、已经出现的替代方案以及过去几年来这个过程是怎样的。

好了，下面交给你了，劳伦 (Laureen)。

谢谢。你需要先取消静音。

劳伦 • 卡宾： 现在这个时间对我来说还很早，所以我要特别欢迎所有处于不方便时区的同事。其他在时间上比较方便的同事，你们肯定会非常感激。

我叫劳伦 • 卡宾，在这次会议上，我会从一个消费者保护最终用户的角度，跟大家谈谈公众如何使用 WHOIS。

可以翻到下一页吗？

我是联邦贸易委员会的一名律师。我在消费者保护国际事务办公室工作，多年来，我和我的机构一直在关注这些问题。但接下来大家要听到的仅仅是我的个人观点。它们不代表 FTC 通过其委员发表的官方立场。你们将听到的仅仅是我，作为联邦贸易委员会中一名高级律师的看法。

请翻到下一页。

另外我也是公共安全工作组的联合主席，倡导这些问题已经有一段时间了。

联邦贸易委员会有一项很好的资源，让全世界的消费者和公众（不仅仅是美国）可以在他们成为受害者或担心有欺骗行为、欺诈或骗局时提交投诉。它就是我们的“消费者哨兵数据库”(Consumer Sentinel Database)。这个数据库每年会收集到数十万条投诉，其中许多来自世界各地的消费者。

可以想象，在看这些投诉时，我们可以得到一些片段，了解公众如何 — 比如说会上网买东西、结识新朋友、获取信息的公众乔 (Joe) 和简 (Jane)，从他们身上，我们可以大致了解到公众如何使用 WHOIS，因为对 WHOIS 的引用就在他们的投诉中。

我所做的事情是，我研究了这些投诉中的一小部分，特别是在 WHOIS 系统的变更生效之后。在这里，我所说的“变更”是

指那些掩盖某些信息（特别是注册人的联系人信息、负责人）的变更。我发现，最终用户使用 WHOIS 的目的多种多样。但本质上，他们都是在寻找可靠的标志。他们想要通过查找 WHOIS 记录来进行审慎性调查，以及跟踪可疑或恶意行为。他们想要找出谁是负责人。有时候他们还想要试着联系他们。有时候我会从这些投诉中得知，他们正在参与诈骗调查，比如说，某个正在试图弄清楚他们是否被骗的人正在给他们打电话。他们会打开电脑，查找可能导致他们接到这个电话的域名。

在实施这些 WHOIS 变更后，消费者注意到，记录中有些信息遭到了删减或存在信息缺失。由于信息的缺乏，他们可能会认为企业不诚实。这种想法可能正确，也可能不正确。顺便说一下，FTC 也收到了这类投诉。但是，他们不会去核实投诉，只是单纯地接收它们，然后把它们作为一个数据点。

所以说人们已经注意到，一些细节信息被隐藏了起来，而这会干扰他们的审慎调查。举个例子，有人投诉称，找不到某个公用事业公司的数据。从这个词云中，大家可以看到不同的人使用它的方式，这些词都是我从自己所看过的投诉中摘下来的。

为了给大家一个大致的感觉，因为我们想要精练一些，毕竟剩下的时间不多了。但是为了给大家一个大致的感觉 — 请翻到下一页 — 大致了解一下，人们使用 WHOIS 来调查的诈骗类型

包括：假冒商品、婚恋诈骗、小狗诈骗。你们应该想不到，世界各地发生了这么多小狗诈骗案！

请翻到下一页。

还有发明诈骗、网络钓鱼。在疫情时代，我们也有冠状病毒钓鱼诈骗。还有技术支持诈骗、假冒公职人员的诈骗、虚假制片、工作诈骗等等，各种各样。

这里我还想要强调一点，人们不仅仅会使用 WHOIS 记录中的联系人信息。从这个意义上说，人们还是比较幸运的，因为那里仍然有一些有用的信息，比如域名创建的时间和地点。以上只是帮助大家大致了解一下，最终用户使用 WHOIS 数据的方式，他们的目的基本上都是保护自己，但他们在投诉中表达了对不为此目的提供某些信息的失望。

下面我要把接力棒交给我的同事加布 (Gabe)。

加布里埃尔 • 安德鲁斯： 好的。下一张幻灯片是我的。

我的发言是代表执法机构的非正式发言。我注意到，尽管需要提供数据，但要从执法机构处准确了解到他们有多少次被不完善的 WHOIS 数据访问弄得心烦意乱极其困难。

此外，执法机构往往会将多个问题混为一谈。有时候他们可能并不是很清楚。但不管是 GDPR 还是《加州消费者隐私法

案》，或者是隐私和代理服务，最终，对警察、调查人员或公共安全官员来说，真正有关系的是他们想要访问数据，但数据并不在那里。

所以，要讨论其中一个问题，就必须从警察的角度来讨论所有这些问题。

请翻到下一页。

我们再深入一点，看看获取数据需要多长时间。这很重要。根据具体情况的不同，它的持续时间和时间线也会不同。

过去，我们在搜索公共数据源后，大概十秒钟后就能得到注册人信息，对吧？这是许多警察根据他们过去的调查经验所习惯的。

现在，如果他们没有得到这些数据，他们可能甚至根本不会知道，在这些数据遭到删减以符合 GDPR 规定的情况下，他们还可以联系注册服务机构来获取未经删减的数据。如果没有适当的隐私/代理服务，他们确实知道可以去联系相关方，而相关方的回应可能是多种多样的。一些注册服务机构会直接回应执法机构对未删减信息的请求，对此我们很是赞赏。

还有一些只会回应当地的执法机构，也就是说，执法机构必须与所请求的机构位于同一国家。如果你们不在同一个国家，那就自认倒霉吧。

还有一些会要求走法律程序。

为方便翻译人员，如果你们听到我说“法律程序”，我指的是法院命令、传票，诸如此类的东西。

如大家所料，这些情况下所需的时间会更长。如果注册服务机构自愿回应，可能也不会再是十秒钟了，而是需要数小时，甚至数天。如果是走法律程序的话，据我估计，获得、送达和收到对法律程序的回应平均需要几天到两周的时间。

如果你们不在同一司法管辖区，并且需要走法律程序，你可能就没那么幸运了。但理论上，如果你是《相互法律援助条约》的签署人，你可以提交 MLAT 请求，然后在六个月后获得数据。

请翻到下一页。

既然谈到了影响，我想说说我们最受影响的流程之一，我们最 — 我们最受影响的职责之一，那就是受害者通知。这里我们以商业电子邮件诈骗为例，它是当今互联网上最常见的犯罪诈骗之一。据估计，去年 2019 年，这类诈骗案造成了 230 亿美元的损失。这个数字似乎每年都会翻上一番。所以，如果今年这个数字接近 500 亿，我丝毫不会感到惊讶。

在这个例子中，大家可以看到，诈骗者正在使用他所注册的域名 ceo@example.com 来冒充 CEO。这是一个相似域名，有时也称为同形异义字，专门针对受害者展开攻击。他会发送一封

电子邮件要求受害者发起电子转账。这就是这种诈骗的运作方式。如果他成功了，那么将有数百万美元不见。过去，作为调查人员，我们会进行反向 DNS 搜索，找到这个恶意域名的注册人，确定他们所注册的其他域名。由于它们是相似域名，我们或许可以从大多数这些域名中推断出真正的受害者是谁，对吧？如果我们能够足够快地做到这一点，如果我们能够行动迅速，那么我们就可以对那些受害者执行进一步 DNS 查询，确定他们的联系人信息，及时让他们知道，他们正成为诈骗者的攻击目标。

但是现在，由于整个过程涉及到多项查找操作，即使这些查找操作只有一点小小的延误，也会降低我们执行关键受害者通知的能力，甚至在我看来，现在已经没有人这样做了。不是因为我们没有尝试，而是因为，获得所有这些额外的潜在受害者域名的第一步，就需要走法律程序，而法律程序现在需要数天或数周才能完成。

我们当然可以这么做。我只是想说，这是现实世界中的一个反应，即使是相对较小的延误，比如说从几秒钟到几分钟，到几天，到几周，它对下游的影响也是非常巨大的。我注意到我没有时间了，而时间是非常宝贵的，所以接下来的时间留给我们的下一位讨论组成员。

乔纳森 • 扎克： 谢谢加布里埃尔 (Gabriel)。接下来发言的是网络安全研究领域的人。格雷格 • 亚伦 (Greg Aaron) 和莱曼 • 查宾 (Lyman Chapin)，有请。

格雷格 • 亚伦： 大家好，我是格雷格 • 亚伦。

请翻到下一页。

最近，我和莱曼 (Lyman) 做了一些有关网络钓鱼的研究，希望借此获得详实的信息，比如有多少钓鱼攻击在发生、在哪里发生等等。

（无声音）

结果，我们发现了近 30 万个钓鱼网址，而这些网址位于 99,000 多个域名中。然后我们找到了它们的托管地。我们查看了事件发生的时间，找出了哪些注册服务机构和托管服务提供商参与其中。

我们发现，钓鱼攻击实际上相当集中。它们往往集中在某些 TLD 的某些地方。发生在一些托管服务提供商的钓鱼事件往往也比其他提供商更多。如果大家访问这里提供的网址，就可以看到详细的研究结果。

其中一项研究发现是，钓鱼域名的使用非常迅速。大多数都在创建域名后的 14 天内使用，很多甚至在创建后的 3 天内使用。

我们还发现，钓鱼攻击问题比所报道的更为严重。每次我们使用一种新的数据源，都会发现其他人所不知道的新的钓鱼攻击。

还有犯罪分子使用的规避手法。

大家在看这些数据的时候，或许可以知道问题的下限是什么，但问题的上限却根本无从知晓。

要想知道有多少钓鱼网站，一种方法是看报道和拦截的数量，这 — 试图找出这些东西 — 我们发现，这有时候很困难。很多这样的数据源都会有非常小的一部分重叠。而且，我们发现世界某些地方根本没有有关钓鱼攻击的数据。由于报道的缘故，中国和俄罗斯等地的钓鱼攻击数据明显不足。

影响我们发现钓鱼网站的其中一个因素就是缺乏 WHOIS 信息。具体有两个问题。下一页。

如果你想衡量严重程度，结果当然取决于你要衡量的是什么以及你是如何衡量的。以 Google 为例，他们的衡量很有意思，因为他们可以明确看到 Chrome 浏览器拦截了多少钓鱼网站。这是一个非常值得关注的衡量标准。这张幻灯片摘自他们的安全浏览专案 (Safe Browsing Program)，其中红色表示已经拦截

的钓鱼网站的数量。之所以说它值得关注，是因为很长一段时间以来，他们使用的衡量方法都没有改变。

大家可以看到，钓鱼网站的数量正在增加。另一方面，恶意软件的数量则在下降。其实这没什么不寻常的。网路犯罪的数量和发生地点往往会随着时间不断变化。导致恶意软件数量下降的原因之一是，一些僵尸网络被撤下。还有一个原因是，犯罪分子现在对操控某些类型的银行恶意软件不如以前那么感兴趣。相反，他们开始使用其他犯罪手法，包括加布刚才提到的商业电子邮件诈骗。

所以说，在试图了解有多少网络犯罪时，结果取决于你衡量的是什么和如何衡量，而且你还需要着眼于全局。对于某些事情，如果你不去衡量，你就不会发现它们。

请翻到下一页。

我们为什么需要 WHOIS 信息？我们需要这些信息，是因为我们想知道一些事情，比如某个域名是什么时候注册的，注册人是谁，等等。这些都是非敏感信息。刚才大家都看到了，注册日期真的很重要。

现在我们遇到的一个问题是限流。也就是说，在一定时间内，注册管理运行机构和注册服务机构只允许你发送一定数量的查询请求。ICANN SSAC 有一篇关于这方面的报告。这样一来，我们就没法获得让我们可以发现更多钓鱼攻击的非敏感信息。

另外，那些负责解决这个问题的人会（或者说过去往往会）查看注册记录中的联系人信息。这一点很重要，因为可以想象，犯罪分子经常会伪造信息。他们不会提供真实的联系人信息。而我们其实是可以对这些信息进行核实的，如果发现信息不实，这就是注册人方面恶意注册的一个表现。

借助这些信息，我们还可以知道某一方是否注册了多个域名，比如通过一些查找和比较手段。但是在后 WHOIS 时代，这个系统不再像之前那么有用了。

不过，我们在报告中看到的一点证实了我们很久以前就知道的一件事，那就是，犯罪分子在注册域名时，他们往往会批量注册，并且我们还发现，这些批量注册的域名不会像之前那样被抓住。在某些情况下，我们可以看到一长串域名，虽然我们发现和拦截了其中一些，但仍然可以看到哪些被漏掉了。

请翻到下一页。

我们关注的另外一个问题是钓鱼攻击的持续时间。这是一些非常棒的数据，由 PayPal、Google 和亚利桑那州立大学的人整理得到，可以说是今年完成的一项重大研究。这些公司之所以这么有洞察力，是因为他们可以看到人们点击了哪些网站，可以追踪人们从第一次访问特定钓鱼网站到最后一次访问的整个过程，并且如果钓鱼事件涉及到 PayPal 付款，他们还可以看到人们是如何受骗的，以及有多少人遭到了钱财损失，等等。

这些数据与其他研究相当一致，包括我做过的一些研究，但它显示的钓鱼攻击时间更短。

从你第一次访问钓鱼网站到某方发现钓鱼攻击，大约需要 8 个小时，而整个钓鱼攻击通常会持续 17 或 18 个小时。也就是说，通常情况下，在发现钓鱼攻击的时候，大部分损失已经造成。大多数受害者已经访问了该网站，那些被骗钱的人已经成为了受害者。

请翻到下一页。

我们还发现，钓鱼攻击中使用的约 60% 的域名都是攻击者自己注册的。

用于实施钓鱼攻击的域名分为两类。一是攻击者直接去购买域名，然后用这些域名来建立他们的虚假网站。除此之外，攻击者也可以使用他们所侵入的域名，这种情况下，他们实际上是用别人，用无辜方的域名在实施钓鱼攻击。

作为攻击事件响应人员，我们想要做的是在托管服务提供商处对这些网站进行处理，继续维护剩下的内容，并防止无辜的注册人遭到任何附带损害。

其实，我们完全可以直接暂停钓鱼攻击者注册的域名，而不造成任何附带损害。

通过我们的衡量方法，我们发现，大约 60% 的域名属于这种恶意注册的域名。

来自 SIDN Labs 和 AFNIC（它们分别是 .NL 和 .FR 的 注册管理运行机构）的团队建立了一个单独的系统。他们使用的方法发现了少量的重叠。他们建立了一个非常复杂的系统，得到的数据是 57%。所以我们两方在这一比例上非常接近，我认为他们的工作做得很好，也很有意思。

下一页。这些是我总结的一些要点。我们的研究显示存在大量滥用注册，但现在我们很难发现它们。其中一个原因是，以前可用的一些数据现在变得不可用，这是很显而易见的一个结论。

在某些方面，联系人数据是区分好域名和恶意域名的关键。它是判断某个域名是否为恶意注册的指标。很显然，域名的注册人或所谓的注册人是很重要的一条信息。

现在，好消息（如果有的话）是，注册服务机构和注册管理运行机构仍然可以访问这些数据。即使其他人都不可以，他们仍然可以。

由于很多钓鱼攻击都是注册这些域名的攻击者自己发起的，这就给注册服务机构和注册管理运行机构继续利用这些数据创造了机会。然而，我们看到的是，在某些 TLD 和某些注册服务机构中，钓鱼攻击屡次发生。

至于 EPDP，其中一个结果是，我们会为数据请求设定一个目标处理时间。有关网络安全的信息请求（比如钓鱼攻击相关信息请求）在 GDPR 中本身便有规定。它们被称为请求数据的合法利益。

不过，5 天的处理时间，有时候甚至可能会延长到 10 天，对我们响应网络犯罪完全没有帮助，因为钓鱼攻击的持续时间往往不到一天。

通过 SSAD 系统获取数据可能比较快，也可能比较慢，而这些获得回复较慢的请求并不能帮助解决当务之急。

所以，钓鱼攻击相关信息请求是自动化测试的理想备选用例之一。这是实施团队需要考虑的。如果这一用例最终得以常规化，那么 SSAD 系统或许可以为响应钓鱼攻击和减少受害提供一些有用的数据。

谢谢。

乔纳森 • 扎克： 谢谢格雷格 (Greg)。

我猜马克 (Mark) 还没有上线。对吗？

>> 对的。

乔纳森 • 扎克： 好的。那么我们继续有请下一位，米尔顿 (Milton)，这样我们才能尽快展开讨论，因为大家都看到了，讨论的氛围相当热烈。就让我们完成这些文稿演示，开始讨论吧。

米尔顿，有请。

米尔顿 • 穆勒 (MILTON MUELLER)： 大家好。我是米尔顿 • 穆勒。我是美国佐治亚理工学院 (Georgia Institute of Technology) 的一名教授。对了，顺便说一下，这个讨论组里的人都来自美国。是不是很有意思？

事实上，一直以来，围绕 WHOIS 的争论主要集中在欧洲和美国在隐私法律上的差异。

可以翻到下一张幻灯片吗？

可能你们还不怎么了解，我为什么会出现在这个讨论组中，实际上，我要谈的是注册人，也就是注册域名的人们，他们享有的权利和权益。大家应该不难理解，为什么域名注册人会对删减某些个人信息感兴趣，对删减敏感的个人信息感兴趣。按照许多隐私法律的规定，他们实际上享有对这些数据进行保护的合法权利和权益。

事实上，我们自己的联邦贸易委员会，也就是劳伦所在的组织，他们提供了很多信息，说明你应该如何不让自己的信息，

比如电子邮箱以及电话号码等其他个人身份信息 (PII)，轻易出现在网络上，以免遭到其他人复制和利用。关于针对 WHOIS 执行 GDPR 规定，到目前为止，我们所做的只是宣扬了犯罪分子和滥用者可以滥用公开 PII 的这一常识。还有就是，一般情况下最好不要把你的电子邮箱和通讯地址随机提供给互联网上的任何人。

尽管如此，在当前的 WHOIS 系统中，仍然有不少的信息，包括注册人姓名/名称、所在国家/地区，有时候你甚至可以查到具体的州/省和城市。所以我们希望，能够找到一些高效的新方法，更快地披露经过删减的数据。

我很好奇的是，为什么一般会员社群对域名注册人享有的权利不感兴趣。我知道他们应该代表用户。我想知道，欧洲一般会员组织在 WHOIS 问题上持有的立场是什么。因为在 EPDP 过程中，我们没有听到 ALAC 对遵从 GDPR 规定的任何支持。

请翻到下一页。

现在，我要引用乔纳森 (Jonathan) 在会议开场时说的话，我们能谈谈当下的实际情况吗？我知道，要确切地知道所发生的事情并不容易，但我们要谨记，现在我们不是要讨论钓鱼攻击是不是坏事，也不是要讨论它们是如何发生的，而是要讨论在按照 GDPR 规定删减数据之前和之后，这些问题是否有所改善。

如果大家去看格雷格刚才展示的 Google 统计数据，从 12 月 15 日到 2018 年 5 月，这基本上是开始实施删减之前的 17 个月，然后再看实施删减之后的 18 个月或 17 个月，你们会发现，恶意网站的数量在之前和之后都有所下降。只不过，后面的下降幅度明显更大。

再来看钓鱼网站，可以看到，在实施删减之前和之后，它的数量都出现了大幅度的增长。

我还查看了一些垃圾邮件数据，尽管很难找到长期的垃圾邮件数据。同样，我也没有发现 2018 年删减数据与问题的规模和范围之间存在任何联系。要在删减与问题变化之间建立任何统计上的相关性是根本不可能的。

所以我认为，你们根据删减与网络犯罪问题之间的数据得出的结论是非常经不起推敲的。

并不是说，在某些情况下，能够快速访问这些数据对执法机构而言没有明显的帮助。很显然，是有帮助的。但另一方面，它也会为威胁创造了机会，是造成问题的部分原因。而且，对于越来越多的钓鱼攻击和滥用性注册，犯罪分子已经学会伪造信息，他们想出了非常聪明的方法来交叉引用和获取虚假的身份信息，而不会被查看 WHOIS 数据的人轻易发现。

关于网络钓鱼问题，最后我想说的是，我在佐治亚理工学院教学生们网络安全的时候，我们做了一个练习，让 5 名学生组成

一个小组，做一封网络钓鱼电子邮件发送给他们的导师，看看能否成功骗到导师。结果，这些学生发现，网络钓鱼域名经常会被托管公司、网络用户和浏览器开发商的各种算法检测到，而这些算法判定网络钓鱼域名的依据包括域名的注册时间、是否匹配某些字符串等等。可能大概有一半的学生发现，他们的网络钓鱼域名在他们能把邮件发到我这里完成作业之前就被拦截了。

请翻到下一页。

重申一下，我们并不是说要完全关闭获取这些信息的渠道。在新的政策制定流程中，我们建立了一种用于提出披露请求的标准化中央系统。但是我认为，我们必须明白，关键在于合规，我们不能忽视这一点。这不是我们可以选择的，你们说呢？我们必须遵从法律。在 EPDP 中，我们辛辛苦苦得出的成果是，我们提出了一项符合 GDPR 的披露机制，根据该机制，许多披露请求必须接受审核，以确定它们是否存在合法利益、请求方是否合法等等。

我就说到这里吧，期待与其他讨论组成员和与会者展开热烈的讨论。

谢谢大家耐心的聆听。

乔纳森 • 扎克： 非常感谢，米尔顿。又是我，乔纳森 • 扎克。我想重申一下米尔顿刚才说的一点，我们要讨论的是当下发生的事情，是对法律的遵从。所以在接下来的讨论环节中，我想我们应该专注于，在实施这部法律后，我们的世界变成了什么样子，而不是重新审视这部法律是好还是坏，或者诸如此类的东西，我们应该专注于数据请求方与数据持有方之间的数据流动关系是怎样的。这才是本次会议的目的。不要再重复 EPDP 已经讨论了两年的话题，而只是回顾总结一下这个过程是怎样的，以及这种关系是怎样的。

说到这点，我认为欧文 (Owen) 是不二人选。他们刚刚就最近的数据请求编制了一份报告。我记不清楚是好久以前了。但是有一场相关的网络研讨会，值得大家去看看。我相信欧文会告诉我们，给我们简单介绍一下，并从数据持有方的角度谈谈自实施临时规范以来的情况，以及过去几年是什么样子的。

欧文，请开始吧。

欧文 • 斯米戈尔斯基 (OWEN SMIGELSKI)： 谢谢乔纳森。

我们来看一下。我这边显示摄像头已经开了，但我在屏幕上看不到自己，你们能看到我吗？

欧赞 • 萨辛： 嗨，欧文。我们可以看到你。

乔纳森 • 扎克： 是的，可以看到和听到你。

欧文 • 斯米戈尔斯基： 好的，很好。我已经习惯看我自己了，但不是 — 好了。下一页。

大家好，我叫欧文 • 斯米戈尔斯基，供职于注册服务机构 Namecheap。同时我也是注册服务机构利益相关方团体政策事务副主席。接下来我要向大家演示的材料是 9 月份注册管理机构和注册服务机构共同举行的网络研讨会的浓缩版本。幻灯片上提供了网络研讨会的链接，点击它可以访问 GNSO 行事历页面的会议演示文稿和录音。我这样做是为了让大家每个人都可以去看一看，了解一下。就我个人而言，我强烈建议大家去看看，因为里面真的有很多信息。

当时，我是与三位同事一起参加那场网络研讨会的，接下来我要演示的内容也是他们与我共同整理而成。他们是来自注册管理机构 Donuts 的艾伦 • 伍兹 (Alan Woods)、来自 .org 注册管理运行机构 PIR 的贝丝 • 培根 (Beth Bacon) 以及来自注册服务机构 Tucows 的萨拉 • 怀尔德 (Sarah Wild)。我要讲的大部分内容都要归功于他们。

请翻到下一页。

我觉得，我们在很多讨论中都漏掉了一点，那就是，GDPR 和数据保护并不是什么新的东西。其根源可以追溯到二次世界大战结束，当时的情况是，在那段时间，国家和其他机构会利用人们的个人信息来描绘和针对许多群体。这些个人信息包括姓名、宗教、种族、性取向等等。所以在经历过那段恐怖的时光后，隐私权在保护个人数据方面变得非常重要，一直延续到今天。这就是为什么数据主体的数据保护问题如此重要，也是为什么我们不能忽视这个问题，因为一些人认为他们有时候会不便提供自己的信息。1948 年，这被写入了《世界人权宣言》。与之相关的还有其他条约和协议，世界上首部国家数据保护法律于 1973 年在瑞典颁布，之后在 1998 年 ICANN 成立之前，还有几十部这样的法律得以颁布实施。

请翻到下一页。

欧洲的所有数据保护法律都提到了 7 个原则，所有这些原则的目的都是为了保护数据主体，但不一定会保护第三方。这里我就不一一细讲了，只是简单说下其中几个，一是你收集信息的目的应该有限。然后，所收集的数据不得超过必要的数据；你必须确保仅把它们存储一定的时间；需要保障它们的安全；以及需要对这些数据负责。

在 GDPR 生效之前，通过 WHOIS 不受限制地访问注册数据就已经违反了这之中的许多原则。

请翻到下一页。

这些只是这里所列问题或观点的一些概览。首先，GDPR 不是什么新发明。虽然它经历了一些微小的变更以加强问责制，但 GDPR 中的规定早在几十年前，就已经存在于欧洲和其他国家/地区的条约中。

WHOIS 也绝不会消失。它仍然在那里。只是现在，它必须遵从法律。我知道，在这次网络研讨会上，大家已经多次重复称，需要 WHOIS 数据来阻止报告。但这并非最好的做法。最好的做法应该是报告给签约方，包括注册服务机构和注册管理机构，或者直接报告给托管服务提供商。他们才是能处理这些问题的人。而你们可以做的是开展事后分析，看看是谁做了什么，以及可以如何阻止他们，你们可以在钓鱼攻击的有限时间结束后来做这件事。

报告和演示并不能解决这个问题。人们需要向我们报告问题，以便我们采取行动。

我重申一下，所有这些数据保护法律，包括加州的 CCPA，我知道巴西也有一部隐私法律，还有其他州也在不断涌现这类法律，它们都赋予了数据主体权利。它们没有向第三方提供任何访问个人数据的权利，也没有规定披露个人数据的义务。

之前，未经删减的 WHOIS 数据为攻击者提供了攻击向量，使得 ICANN 社群十多年来一直忙于应对这类问题，包括域名劫

持、垃圾邮件、网络钓鱼、电话诈骗、虚假续订通知等等。其实，我们多年来一直在谈论的所有事情都可以通过保护注册数据不被任何人完全访问来解决。

同样，正如我们一再听到的，总的来说，滥用域名的情况并没有加剧。相反，它还有所缓解。并且，在 2019 年新冠疫情期间，也没有出现总体加剧的情况。

请翻到下一页。

这里我只是拟了一个大纲。对于那些想要提出数据请求的人，这是在提出数据披露请求时，应该向注册管理机构或注册服务机构提供的信息的最低要求。它是我们根据 EPDP 第 2 阶段工作《最终报告》以及注册服务机构和注册管理机构整理的最佳实践总结而成。这里有一个链接，点击它可以直接访问注册服务机构利益相关方团体的网站。这些只是签约方在审核披露请求时所需的基本信息，有了这些信息，他们才有可能开展平衡测试，看看是否应该应请求进行披露。如果没有这些信息，那么将导致整个流程需要更长的时间。

确实，有时候，注册服务机构和注册管理机构收到的投诉根本没有提及问题域名，或者未说明请求方要主张什么合法权利，或者他们想要获得哪些数据元素。而这，会拖慢在整个流程。所以，你们需要做的只是提供注册服务机构或注册管理机构需要的一切信息，这样他们才能配合，才能更快地做出披露决策。

请翻到下一页。

这是我们做的一个信息概览，这些信息都是我们为这次演示所整理的，是一些注册服务机构和注册管理机构自愿提供的数据。它们代表了小、中、大型注册服务机构和注册管理机构，同时代表了全球多个地理区域。数据的涵盖范围很广，有些注册服务机构报告的披露请求只有 30 条，而有些报告的多达 3400 条。注册管理机构报告的数量较低，虽然在刚开始执行 GDPR 后报告的数量较高，但自那以后就趋于稳定。

这里的一些关键要点是，处于管理之下且接受披露请求的域名只有总数的 1% 不到，并且它们的披露情况根据删减类型的不同而有所不同，因为不同签约方在实施临时规范和其他规定时做出了不同的调整。

另外我还想强调的是，如果使用 SSAD，ICANN 要求报告的指标会多得多，这些指标会同时报告给 ICANN 和社群。所以在 SSAD 投入使用后，对于收到了哪些类型的披露请求、谁负责处理、结果如何等等问题，我们都会有一个更好的了解。

请翻到下一页。

这里是我们总结的一些处理结果。大家可以看到，对注册管理机构而言，拒绝和重定向的请求大约占了一半，而对注册服务机构而言，大约有三分之二的请求都遭到了他们的拒绝或重定向。

我所说的“重定向”是指，注册管理机构告诉请求方去联系注册服务机构或以非法为由拒绝。其中涉及到平衡测试。

除此之外，导致数据得不到披露的还有一些其他的原因，比如域名受隐私服务保护，或者域名不是在这个注册服务机构或注册管理机构注册的。

请翻到下一页。

那么，我们都提供了哪些类型的数据？在我们披露的数据中，三分之一为注册人数据，三分之二为注册人的管理和技术数据。一般来说，如果拒绝披露数据，标准的做法是提供相应的理由和说明。但是，如果注册人使用了隐私/代理服务，那么提出数据披露请求便不是适当的做法。隐私/代理服务在这方面有它们自己的流程和程序。

请翻到下一页。

一些注册服务机构因为拒绝披露请求收到了一些申诉。注册管理机构则没有收到过这类申诉。大家可以看到，注册服务机构报告的数量非常低。通常，这些申诉都与通过不当机制提出披露请求相关，一般我们的做法是对他们进行教育宣传，或者向他们说明那种情况下拒绝请求的原因。值得注意的是，在这些申诉中，没有导致披露决策或不做出披露决策的结果被推翻的申诉。

请翻到下一页。

这是关于所提出的请求类型的一些信息。大家可以看到，大约四分之三的请求来自执法机构，抱歉，应该是来自 IP，约 15% 来自执法机构，剩下的均来自其他方，包括安全研究人员提出的请求、未提及域名（难以识别）的请求以及所涉域名并未在该注册服务机构或注册管理机构注册的请求。

请翻到下一页。

在提出请求的请求方中，我发现，平均每个请求方会提出四条请求。也就是说，有很多请求方都提出了多次请求。事实上，在我们收到的请求中，45% 都来自某一个请求方，这在请求总量中占了相当大一部分。

我认为这是 — 请再翻到下一页。

这是一般情况下的响应时间。总的来说，我们的响应时间不到三天。其中，注册管理机构的响应时间比注册服务机构要短，这是因为，很多时候，注册管理机构都会建议请求方联系注册服务机构，后者更便于掌握数据或做出披露决策。

我要说的就到这里了。希望我讲的不是很快，我只是想要确保后面有足够的时间讨论。

谢谢。

乔纳森 • 扎克： 谢谢欧文。我知道时间很短，而你要谈的内容很多。所以我很感激你能快速讲完。你们的数据非常有用。

欧文 • 斯米戈尔斯基： 还请大家去看一看 9 月份举行的那场网络研讨会。实际的会议有一个半小时，我刚才是对它进行了压缩。那场会议的讨论很热烈，也有很多有用的信息。谢谢。

乔纳森 • 扎克： 那肯定的。在场的工作人员，如果你们能找一下那场会议的 Zoom 录音链接，然后把它发到聊天室里，那将会很好。我认为，它可以为我们的讨论提供很好的背景信息。感谢签约方整理这些数据。

另外，麻烦工作人员把演示文稿往后倒一点，因为马克 • 斯万卡雷克 (Mark Svancarek) 已经上线了，我希望他能跟我们简单说说。

马克，废话不多说，开始吧。

马克 • 斯万卡雷克： 谢谢大家。能听到吗？

乔纳森 • 扎克： 能。

马克 • 斯万卡雷克： 抱歉。我的闹钟坏了。太不专业了，是吧？

大家好，我是马克 • 斯万卡雷克，供职于微软，我要跟大家谈的是，在微软，我们如何看待网络犯罪，以及与 WHOIS 和 GDPR 相关的一些事宜。

我会尽量讲快点，这样我们就可以快点（笑声）开始讨论了。

我在聊天室里发了一些东西。这是微软最新发布的《数字防御报告》(Digital Defense Report)。这是我们第一次做。报告内容非常全面，阐述了我们如何看待网络犯罪的现状。

最近有很多关于网络犯罪是呈上升还是下降趋势的讨论。我不知道大家为什么要争论这个。事实上，它正在上升。所有类型的网络犯罪都在上升。所以对它的防御仍然是一项高度优先的任务，我们也为此付出了大量努力。

WHOIS 数据集是我们用来处理各种网络犯罪的工具之一，包括企业网络犯罪、消费者欺诈、反盗版、国家行为者威胁评估等等。

抱歉。

对，我没有提交幻灯片。我很抱歉。因为我在提前查看幻灯片时，我发现好像只有米尔顿提交了。所以我还以为，这场会议更多的是讨论。

所以 — 抱歉。

不管怎么说，现在，对于 GDPR 下的 WHOIS，我们面临的挑战是，我们还没有真正开发出一个系统，一个使我们可以在法规允许的最大程度上访问数据的系统。虽然我认为，在小组中对此展开进一步讨论将会很有帮助，但事实上，我们已经收到了一定数量的法律信息。而在小组内部，我们对这些法律反馈的实际意义尚未达成共识。这涉及到准确性、必要性等诸如此类的东西。

所以我想，如果大家去看一下 9 月份的那场网络研讨会，在会议大约 34 分钟的时候，他们提出了平衡测试，我觉得大家应该会发现，它与我们从 Bird & Bird 收到的有关“必要性”含义的反馈大相径庭。我这里有一些信息，大家可以看一下 — 哪儿去了？我很抱歉。我没有把链接发上来。我以为我发了。基本上 — 抱歉。各位，真的很抱歉。

我马上把这些东西发到聊天室里去。但基本上，它归根结底是必要的 — 这里我需要引用我自己的原话。

我们继续吧。

天哪，天哪，天哪！趁着找链接的机会，我想说的是，我们都听说过诸如 UDRP 这样的争议解决方案的存在，这意味着在 WHOIS 下披露数据永远都是不合法的。但事实并非如此。

乔纳森 • 扎克： 嘿，马克。我是乔纳森。

马克 • 斯万卡雷克： 我马上就回来。

乔纳森 • 扎克： 其实你不需要把链接发上来的。如果你真的有什么重要的观点想说，那么去找链接没什么问题。但是我们也可以直接开始讨论。

马克 • 斯万卡雷克： 那我们开始讨论吧。稍后我会找到这些链接的。

但问题是，根据我们收到的法律反馈，有很多人认为 SSAD 的开发方式是唯一的。然而现实情况并非如此。现实情况是，我们还有多个其他选择，只是我们选择不去采纳它们。

这条路 —

乔纳森 • 扎克： 谢谢马克。我想，我们真的有必要遵循不去重新审视这些问题的决定，而是要实际去了解一下这些请求都是什么样的、处理时间如何等等。这就是欧文提供的数据如此有用的原因。

我知道，大卫 • 泰勒 (David Taylor) 从请求方的角度整理了一些数据。

但我觉得，现在我想做的是让大家知道，GDPR 已经成为既定事实，它的实行已经成为既定事实，EPDP 建议的实施也已经

成为既定事实，所以我们要考虑的是，数据请求方与数据持有方之间的沟通渠道（抱歉，没有想到更好的词）是否能很好的运作？

我认为这才是我们接下来应该讨论的东西，即，目前两方之间的交流是什么样的。所以，欧文提供的数据真的很有用。

因为，举个例子，在文稿演示前期有人提出了一件事情，我记得是加布里埃尔提的吧，他说，在我们发现网络钓鱼诈骗时，诈骗已经结束了，这意味着，比如在收到投诉后，签约方根本不可能及时把数据返回给你。

所以我认为，我们应该围绕这类数据交换的实际情况，展开一场真正的对话。

我看一下。好的，其中一个得到大量讨论的话题是，DAAR 数据似乎表明 DNS 滥用在很大程度上呈下降趋势。然而，其他数据似乎表明它呈上升趋势或者以不同的方式上升，等等。

有人愿意接受这个观点吗？鲁克 • 瑟弗 (Luc Seufer) 在提问窗格中提出了一个问题。为什么这两个不同的数据集会得出这种互相矛盾的结果呢？为什么对于 DNS 滥用的趋势走向，我们不能得出一个确切的答案呢？

格雷格 • 亚伦： 你好，乔纳森。我是格雷格。作为 DAAR 系统的设计者和开发者，我可以谈谈这个问题。

其实 DAAR 系统所做的工作是，将多个不同的域名黑名单中的数据进行汇总。它会查看涵盖诸如网络钓鱼和恶意软件等特定类别域名的黑名单。

一般情况下，按照我们的预计，它会随着时间起伏波动。在下降了一段时间后，它可能会再次上升。这是规律。

它衡量的是来自特定数据源的特定事件。不过，我们发现，新的规避手法可能会导致大家看到的域名数量减少。我们并不知道，限制 WHOIS 的数据的披露会产生什么影响，会对黑名单拦截产生什么影响。不过，一些数据源已经对它进行了衡量，而且还有一些出版物表明，如果寻找恶意攻击者变得更加困难，那么被拦截的域名就会减少。这是可能的影响之一。

但是，这并不意味着，网络犯罪的数量下降了。它只是意味着，你能找到的恶意域名减少了，你能在黑名单中找到的域名减少了。

欧文刚才说，总的域名滥用正在减少，这可能是根据特定情况和特定数据源进行衡量的结果。

不过，无论你怎么衡量，它都是很多的。另一件要提醒我们自己的事是，给定黑名单中的域名数量并不能衡量所造成的损害，也不能衡量所涉及的风险。以商业电子邮件诈骗为例，这

些诈骗造成的平均损失金额一直在上升。所以，如果域名的数量跟以前一样多，那么给受害者造成的损失会更大。

我认为，这真的取决于你要衡量的是什么以及如何衡量。其他指标表明它在上升。DAAR 只是采取了一种特定的方式进行衡量。我不认为这可以代表整个生态系统的情况。谢谢。

乔纳森 • 扎克： 谢谢格雷格。西奥 • 吉尔茨 (Theo Geurts) 问道：注册服务机构所披露数据的质量如何？对调查有用吗？

我们听到很多人说，由于缺乏准确性以及存在隐私和代理服务等等，数据的质量已经开始走下坡路了。你们真的能 — 我想，就像米尔顿问的那样：你们真的能将所面临的困难归因于 GDPR 合规带来的改变吗？这个问题应该是问网络安全研究领域和执法机构的人的。

加布里埃尔 • 安德鲁斯： 大家好。我是加布里埃尔。请容许我插两句，简单回答一下这个问题。

乔纳森 • 扎克： 有请。

加布里埃尔・安德鲁斯： 我认为，虽然响应的质量会有明显的不同，但还是值得去争取的。只有当它回复什么信息也不会提供给你的隐私/代理服务时，这个响应才真正一文不值。但我们发现，即使犯罪分子在注册人信息上撒谎，或者使用的是遭到泄露的支付凭据等等，这些都是数据点。你永远不会知道，哪个数据点会成为撬开公开调查的关键。所以，与其什么数据也没有，我宁愿去争取哪怕是欺诈性的注册人数据。不过，很明显，在域名注册时对数据的验证越严格，对我们越有利，而对犯罪分子越不利。

谢谢加布里埃尔。

丝黛芬妮・裴琳 (Stephanie Perrin) 提了一个问题：对于有效数据被窃取和用来替代犯罪分子数据的频率，我们是否有相应的统计数据？我们已经收集了历史数据，其中很多仍然很有用。

格雷格・亚伦： 我是格雷格。这个问题我可以回答。你好，丝黛芬妮 (Stephanie)。

乔纳森・扎克： 很好，谢谢。

格雷格・亚伦： 我的意思是，我看过这些年来遭到滥用的数百万域名的联系人数据。我发现，一般情况下，犯罪分子不会提取和利用他人的

数据。他们往往会直接伪造数据。有些人伪造的比较好，有些人则不然。但就我的个人经验而言，犯罪分子使用被盗用数据的情况相对少见。

乔纳森 • 扎克： 好的。谢谢。

我觉得我应该问一下，你发言的时候能不能把摄像头打开？我们要让尽可能多的面孔出现在这些线上会议中。所以，你在回答问题的时候如果能把摄像头打开，那就太好了。我知道这需要你来回地操作，但理想情况下，大家可以看到你的。

福尔克尔 (Volker) 说：格雷格的意思似乎是，由于损害已经造成，在收到报告时再撤销域名没有任何好处。这似乎有些违反常理。

格雷格 • 亚伦： 不，我觉得福尔克尔误解我的意思了。从我刚才展示的那张图表中，大家可以看到，撤销域名会有增效的作用。没错，网络钓鱼是持续时间最短的网络犯罪类型之一。不过，在其他问题上，暂停犯罪分子注册的域名会给你带来更大的好处，所以这项操作非常有用。

但是，问题在于，事后缓解与防范于未然是有区别的。从数据中我们可以看到，犯罪分子总是会去某些特定的地方注册域

名。如果他们的域名遭到暂停，他们会再去注册其他域名。重复犯罪活动确实是我们面临的一个问题。如果能及早发现和防范这些重复犯罪活动，那将会很好。

所以我想说的是，暂停域名没有任何价值吗？不，它绝对值得我们去做。

重申一下，我们的目的是保护那些受害的人。

米尔顿 • 穆勒： 我能插两句吗，乔纳森？

乔纳森 • 扎克： 当然可以，米尔顿。请讲。

米尔顿 • 穆勒： 重申一下，我认为我们真的需要关注 WHOIS 数据删减前后的情况。这才是我们要讨论的问题。我不认为它跟说网络钓鱼是个问题有什么关系。这点我们都知道。

问题是：在打击网络钓鱼或其他形式的网络犯罪时，我们有多依赖对 WHOIS 数据的公开访问权限？

在我看来，犯罪分子想出了相当可靠的方法来避免被发现，真正能阻止钓鱼域名发起攻击的大都是暂停域名，以及能够检测到攻击模式并迅速拦截它们的算法。我不清楚 WHOIS 数据的

存在或缺失是否与此相关。但是，大家再来看一下数据，我们会发现，这些问题在 WHOIS 变革前后并没有统计学上的相关性。我们应该记住这一点。

我认为，你不能简单地说，我们喜欢拥有这些数据的访问权限。但是当你可以随意、开放地访问这些数据时，网络钓鱼仍然是个问题。它是一个日益严重的问题，而且发展的速度会比现在更快。

所以，我想再次呼吁大家，如果可以的话，把中心放在因果关系上。

乔纳森 • 扎克： 非常好的问题，米尔顿。有人想从执法机构或网络安全领域的角度就此说几句吗？

加布里埃尔 • 安德鲁斯： 我可以补充一点，这些数据的缺乏会对调查产生不利影响。发生这种情况的原因有很多，但那涉及的领域可能更广。

我想提醒大家，同时重申一下我之前的言论，那就是，我们的职责不仅仅是找到攻击者，有时候还包括迅速通知潜在受害者。这是一个真实世界的例子，在这个例子中，我们确实受到了影响，因为我们不仅需要 DNS 系统中的数据主体标识符，还需要与被确定为攻击对象的受害者相关的身份信息，我们假

设它们都是有效数据。但如果我们无法迅速得到这些数据 — 本来，有了这些数据后，我们就可以在当天或第二天通过电话告知潜在受害者，他们的邮箱帐户可能会遭到入侵，而他们会成为被攻击的目标，这类通知很重要。但是如果我们无法迅速得到这些数据，那么我们就做不到这一点，从而导致世界各地的公众受到损害。

乔纳森 • 扎克： 加布里埃尔，你是说，利用这些数据联系无辜者比追踪犯罪分子更有价值吗？

加布里埃尔 • 安德鲁斯： 我觉得这个没法衡量。如果可以的话，我只能说，它对两者都有用。我很难对正在发生的事情做出广泛、笼统的断言，因为我曾经尝试过收集数据，但后来发现，让调查人员从百忙之中抽出时间来回复我真的太困难了。比如说，我尝试了 82 次获取注册人信息，成功了 42 次。对吧？他们不会追踪失败的情况。更不用说再回过头来向我提供我知道将在这里非常有用的一些事实了，那是非常困难的。

但我可以说的是，我在收集这些数据的过程中，让我最印象深刻的一件事是，一些调查人员在试图做正确的事、试图通知那些可能受到伤害的人，但却发现他们受到了阻碍时，他们所感

受到的沮丧。这并不是说，他们不能以某种方式去探索其他途径。

而是说，这是最快速的方法，过去给他们带来了很大的帮助，但现在却不然。我只是想阐明这一点。

接下来你继续吧。

乔纳森 • 扎克： 谢谢，加布里埃尔。

欧文，我知道，最近签约方关于数据访问的演示为最好地规范化披露请求奠定了基础，有助于加快规范化进程等等。那么，有没有能够说明数据请求方采取这种做法的任何例子或数据？

另外，这与更有可能更快地获得数据是否存在任何相关性？

欧文 • 斯米戈尔斯基： 谢谢乔纳森。大家好，我是欧文 • 斯米戈尔斯基。我真的无法从中得出任何结论。很明显，它是一个有限并且不一定全面的数据集，但签约方的经验是，在收到提供这些额外信息的披露请求时，他们的处理速度确实会更快。他们能够更快地开展适当的平衡测试。但仅仅因为你提供了所有必要信息并不意味着，你提出的请求就能通过平衡测试。至于是否有更缓和的方式来争取，而不是直接获取数据。我想说的是，这可能需要考虑到很多问题和因素。

它确实能够加快处理流程，让你能更快得到结论。大部分数据显示，大多数请求都关乎商标侵权。所以一般来说，这并不是需要清除僵尸网络的紧急情况之一。你还可以选择其他途径，比如 UDRP、URS 或其他不需要使用相关数据的类似机制。这就是一种比较缓和的方法，同时，也正是因为有比较缓和的方法来处理它，它的平衡测试必定会以失败告终。

乔纳森 • 扎克： 欧文，在你看来，未来平衡测试是否应该继续完全基于个案，还是说可以采取某种方法，比如，把所有签署了 DNS 滥用框架的人聚集在一起，让他们共同建立一种决策树模型，使平衡测试对那些试图从签约方处获得数据的人来说不那么像一个黑匣子？

欧文 • 斯米戈尔斯基： 谢谢乔纳森。又是我，欧文。

未来会发生什么，我真的说不准。对于哪些是允许的，哪些是不允许的，目前仍然有很多模棱两可和不确定的地方。已经提出的一些指导意见是，不，某些东西不一定要弄成自动化。并且，数据披露请求中有太多的未知因素。

我知道，有些人在说，美国国会应该通过一些法律，规定可公开访问 WHOIS 数据。但是，对于像 Namecheap 这样在全球拥有数百万客户的大型注册服务机构，我们不能百分之百肯定地

说，因为这个人不在司法管辖范围内，不受数据隐私法律的保护，所以披露这些数据会使我们承担潜在的民事和刑事责任。这不是可以轻易找到放之四海皆准的方法的事情。一些注册服务机构可能规模比较小，或者只专注于某个地区，或者采用不同的商业模型。

我相信，它会随着时间的推移不断发展，SSAC 肯定会通过政策制定流程来发展和改变它，但现在就预测它将如何发展还为时过早。

谢谢。

乔纳森 • 扎克： 谢谢欧文。我猜应该是关于同一个问题，洛里 • 舒尔曼 (Lori Schulman) 问道：关于收到了多少请求，其中有多少请求的处理结果是披露数据，你是否愿意分享一点 Namecheap 的具体经验？

欧文 • 斯米戈尔斯基： 你好，乔纳森。又是我，欧文。这不是我能在这里讨论的。目前我没有权限访问那些数据。

乔纳森 • 扎克： 很好。谢谢。

我知道你们在提问窗格、在聊天室里展开了讨论，我也一直在努力关注你们提的所有问题，试图弄清楚大家都在说些什么。

马克 • 格拉汉姆 (Mike Graham)，如果你在线上的话，我知道你提了一个关于数据删减变化的问题。你要打开麦克风，跟我们分享一下你的问题吗？因为你的问题已经在很前面了。

我并不是想让你为难。

没错，你能打开麦克风吗？或者说，我们的工作人员能允许马克 (Mike) 打开他的麦克风吗？

马克尔 • 格拉汉姆 (MICHAEL GRAHAM)： 现在可以了吗？

乔纳森 • 扎克： 可以了。谢谢。

马克尔 • 格拉汉姆： 抱歉。我只是分享一点工作和费用方面的信息，很快就好。它产生影响的方式有两种。一种是发现信息，这样我们就能确定某个域名是否遭到了欺诈性注册并被投入使用，或者它可能是由某个与我们公司有关系的人注册的，仅仅是无意误植域名的结果。

毫无疑问，在后一种情况下，我们明白，很多互联网用户上网的目的其实很简单，但他们做的事情可能不仅会损害我们联系

消费者的能力，还会（听不清）他们这样做并成为良好网民的能力，然后对企业而言，这其中的调查成本，也就是为找到该信息所需的额外成本，将会是一笔巨大的费用。至于真正的滥用 — 这种滥用不一定是网络钓鱼，在某些情况下，它对我们来说可能是网络钓鱼，但在另一些情况下，它就是互联网上的假冒行为。调查成本已经大幅上升。在某种程度上，这不仅是我们的损失，也是消费者的损失，不仅是经济方面的损失，还损害了他们对能在互联网上找到所需信息的信任。这才是真正让我们担心的事情，我们希望，他们能够找到他们想要的东西，而不会被这些日复一日的骗局所欺骗。

乔纳森 • 扎克： 谢谢马克尔。

成本问题是一个很复杂的问题，因为很明显，数据请求方群体有时候对施加给签约方的成本并不敏感。大家知道，为了满足请求方需求所产生的成本。

所以说，如果遵从法律只是经营生意的一项成本的话，我认为这也是一个复杂的平衡问题。

伊丽莎白 (Elizabeth) —

米尔顿 • 穆勒： 在这个问题上，我能插两句吗？

乔纳森 • 扎克： 可以，米尔顿。请讲。

米尔顿 • 穆勒： 从某种意义上说，成本才是最重要的，因为 20 年来，请求方不仅享受了“免费的午餐”，可以说还得到了 ICANN 制度的贴补。而我们，基本上是与域名注册人签署了一份附和合同，上面规定，如果你想要注册域名，那么在不需要你同意、你也没有任何发言权的情况下，您必须公开提供自己的个人身份信息，让全世界任何需要它的人都可以访问。这会给注册人带来成本，但却贴补了访问信息的人，他们之中的一些人会通过收集和出售这些信息来赚钱。

现在，我们开发了 SSAD，这会导致成本以一种更公正、更有效的方式在各方之间分摊。如果你是一位需要请求大量数据的请求方，我们都能想到，大多数的请求来自哪些公司，在这方面，我觉得欧文的数据很有帮助，大家知道，你们才是产生系统成本的人。可以说，你们才是成本制造者，所以你们应该付出更多。你们应该支持系统，比如通过支付用户产生的费用或者某种等级认证费用等等，以此来抵消披露你们所请求数据产生的成本。

如果数据的披露速度如你所期望的那样快，很显然，它会给签约方带来巨大的成本，因为他们必须安排人坐在那里评估这些请求。当然，你可以通过自动化来避免其中某些成本，但如果你对请求性质的评估不当，那么自动化也可能是非法的。

所以，乔纳森，就像你说的，这确实是一个复杂的挑战，我认为，对于今天这个讨论组中的各位，我们最好能更清楚地意识到，成本是如何在不同利益相关方群体之间以一种平衡的方式分配的。

乔纳森・扎克： 谢谢米尔顿。

娜塔莉・勒罗伊 (Natalie Leroy) 问：如果请求方能提供商标注册的证据，大多数欧洲注册管理机构都会提供符合 GDPR 规定的数据披露服务。gTLD 或其他 ccTLD 是否会考虑采用类似的模式？这将极大地帮助我们开展执法工作。

欧文，即使你现在不知道答案，你也可能是唯一能够回答这个问题的人了。

欧文・斯米戈尔斯基： 抱歉。我刚才在看聊天室里的内容。你问的是哪个问题？

乔纳森・扎克： 抱歉，娜塔莉・勒罗伊。是提问窗格最下面的那个问题。

欧文・斯米戈尔斯基： 我不知道 — 谢谢。我是欧文。

我不确定是否有其他 gTLD 或 ccTLD 采用类似的模式，但是，随着这个过程的推进，随着我们开始使用 SSAD，我们可能会找到一种认证用户的方法，比如针对特定的 gTLD，或者诸如此类的东西。

EPDP 第 2 阶段工作《最终报告》的发布就是我们的起点。我们在紧迫的时间下完成了所有事情，把所有东西都放了进去。无论内部还是外部，都有很多参与者想要比我们更快地完成，所以我们在有限的时间内尽了最大的努力。

我认为，随着 SSAD 模式的发展，我们完全可以把这作为以后的一个建议。我认为，如果它获得了一致同意并且符合法律规定，那么（听不清）肯定更容易。

谢谢。

乔纳森 • 扎克： 谢谢欧文。

希望这能回答你的问题，娜塔莉 (Natalie)。我觉得，这个问题涉及的范围太广，不是我们今天能够解决的。

劳伦要求回应米尔顿。劳伦，请讲。或者，能否麻烦工作人员开一下劳伦的麦克风？

劳伦 • 卡宾： 我想我已经取消静音了。

乔纳森 • 扎克： 好的，很好。

劳伦 • 卡宾： 谢谢。米尔顿刚才说这些信息是一把双刃剑，对此我表示赞同。人们可以把它用于不好的目的，这一点毋庸置疑。事实上，米尔顿，我们在投诉数据中也看到了这一点。

但另一方面，DNS 是一种公共资源。米尔顿举了一个例子，称有些人会把这些信息收集起来用于恶意目的，这是违反法律的，相信大家对此都没有异议。

但是，GDPR 并不保护法人实体的数据。我期待当前正在开展的有关这方面的政策制定工作，因为公众确实有权知道法人实体的信息。如果稍微改变一下，允许用户发现域名背后的任何非个人实体，这将在很大程度上帮助公众和执法机构展开调查和审慎性调查。

正如我们必须提供某些信息（无论是驾照还是营业执照，而且其中一些信息还必须公开）才能使用公共资源一样，对与法人实体相关的法律信息也应该这样做。

乔纳森 • 扎克： 谢谢劳伦。

聊天室里还有很多其他问题，我们的工作人员会把它们收集起来，然后我们会设法回复大家。很遗憾，现在我们已经没有时间了。这真的是一场很愉快的讨论。有时候保持专注太难了。杰夫 (Jeff) 问道全体会议的目的是什么，我不确定。但理想情况下，我们对 ICAN 政策变化前后的实际情况了解得越多，就越能更好地确定下一步需要采取的行动。我认为这就是这次讨论的目的，即，尽可能地了解这种对现状的改变给数据流动和网络安全研究机构保护消费者所需的数据的可用性带来了怎样的影响。

希望我们能稍微往实况调查方面使劲。显然，我们还需要进行更多的实况调查。聊天室里还有很多问题。之后我们会看看可以如何解决他们，但今天，我们没有时间了。现在我这边是凌晨 3 点，所以我可能说不出什么幽默的话来了，我只是想对所有做演示和所有参加这次讨论会的人说声谢谢。我们会去看聊天室里的内容，并以此作为日后讨论会的话题。

再次感谢大家。本次会议到此结束。

[会议记录结束]