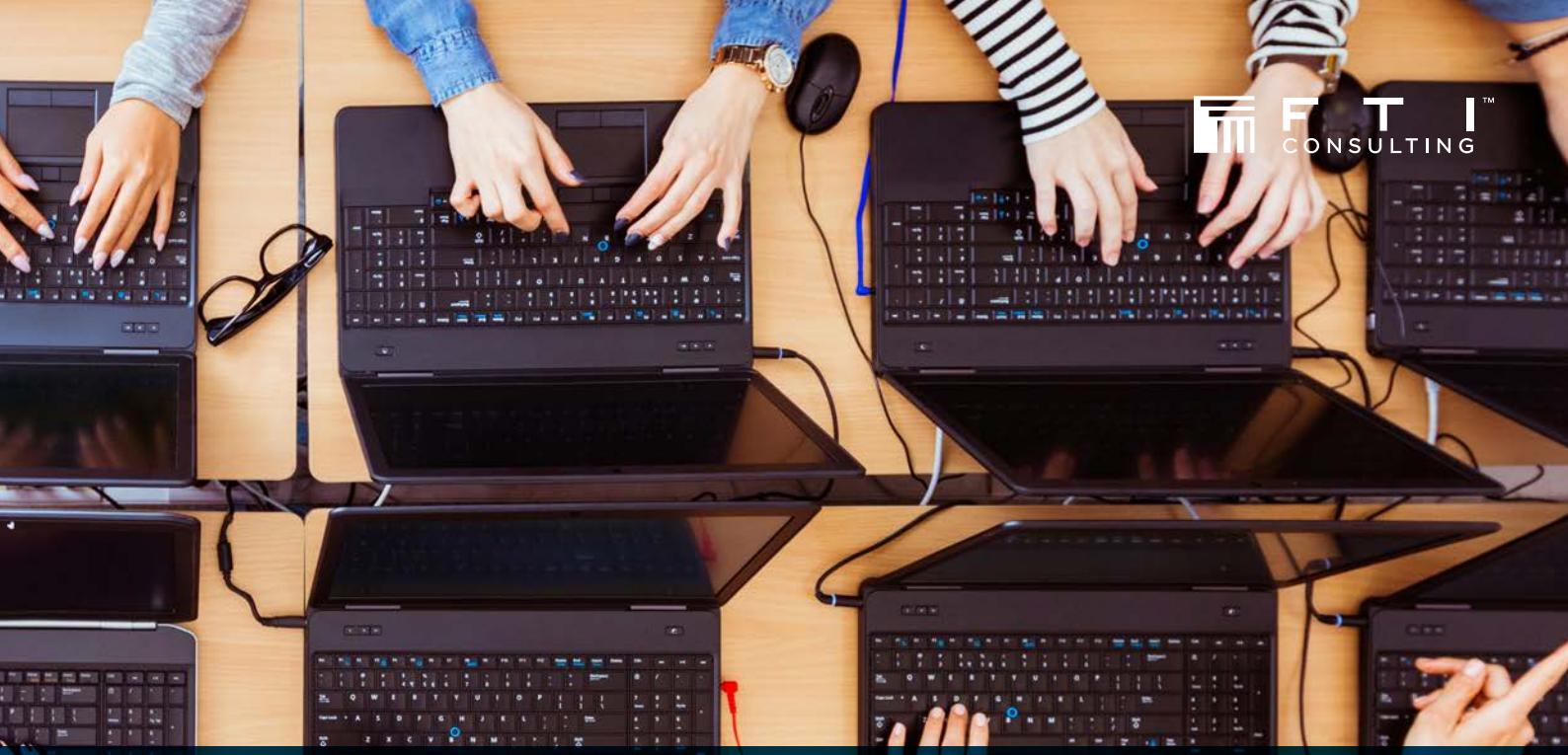

ECONOMIC & FINANCIAL CONSULTING

Desktops and the Licensing of Potential Use

Why are desktops treated as single-user devices and subject to simplified user counting rules, when they're as capable of servicing multiple users as servers?

A common argument in software licensing is whether a license is given in respect of actual use or potential use i.e. whether a license is required even if the licensee makes no use of the software. This depends upon what the license agreement says but it is not unusual to find customer and publisher having different views.

This issue was relevant in a recent, now settled litigation in which one of the points of contention was the counting of user licenses for software that was installed on servers. The customer's objection to the publisher's counting method was that it included users who in the customer's view:

a) were unable to use the software;

b) would never need to use such software; and/or

c) had no knowledge of the software, the server's existence, or how to connect to it.

The difference between the two sides' counts was millions of dollars.

Setting aside the license agreement and the contractual aspects, there was an interesting inconsistency between the approaches to counting potential use for servers and desktops. Users for server-based software were counted based on the security groups to which users are assigned to determine their ability to access the servers and/or the software installed upon them. Desktops and workstations on the other hand were treated as having, and capable of having, only a single user.

This is often not the case. While it may be unlikely for desktops to be used by multiple users, it is not impossible and there are circumstances where it might be routine, such as the use of a desktop in a library or a research lab. Sharing of login credentials aside, the administration of user access for desktops and servers is more alike than might be expected.

Desktops and Servers are more alike than you think

Generally, any user in an Active Directory (AD) domain can, by default, log on to any computer in the same domain. If you try to log in to a colleague's device with your own credentials, you will likely see this in action. The reason for this is that users in AD are automatically added to the "Domain Users" group which is, by default, present in the local "Users" group on a domain-joined desktop. These local users can log in to the desktop. This behaviour is enabled by default but can be restricted by IT. The best way to do so, particularly in large organisations, is to

use Active Directory security groups. This is the same control that usually constrains access to servers. With this in mind, the differing treatment of potential use between servers and desktops is not as well-founded as it seems.

It is understandable why it is generally accepted that desktops are single-user devices. In contrast to servers, which are frequently used to provide access to shared resources, desktops are aimed at individual consumption. On the desktop this manifests in lower performance capabilities and limitations in software, some of which can be overcome. However, the arguments for counting licenses are often focused on the possibility of something happening, so it is jarring that such a broad assumption is generally accepted.

It may simply be pragmatic for vendors to treat desktops this way because in most cases the likelihood of significant multiple users is small compared to the potential proliferation of user access to servers. But if the reason is pragmatism, it rather undermines the assertion, in relation to servers, that potential usage is a matter of principle. And it suggests that robust evidence on limits to server access ought to be taken into account by vendors whenever licensing on potential access is being claimed.

To be clear, there is no reason why software should not be licensed on a potential usage basis. However, given the potential for misunderstanding, and the scale of findings that might arise, it is important for this to be set out clearly in the license agreement, and it usually is.

It is also important for customers and publishers to have a very clear view of exactly how a program is installed and how the license mechanism, if any, operates in relation to individual user profiles. Except for those publishers whose programs are almost wholly desktop-based, this level of detail is not usually considered by either customers or publishers.

The implications for publishers, auditors and customers

Publishers

For publishers, licensing rules must be applied consistently and fairly, particularly in the context of a software audit. Customers should be expected to exert as much control over their desktop estate as their server estate, not only because of the treatment of potential access but also because it reduces the risk of over-deployment more generally and the associated knock-on effects, such as users' ability to install their own software which is a key route by which pirated software enters organisations.

Software Auditors

For software auditors, there should be more scrutiny of which users are actually accessing desktops. There's a wealth of un-mined information contained in desktops such as Windows' logs of user login activity that can be used to understand user behaviour across an estate and its implication on licensing. For example, it could be used to raise red flags related to the sharing of login credentials if analysis of such logs discovers the same user ID logged on to two separate machines concurrently in different geographic locations.

Aside from counting licensable users, a more in-depth approach is especially relevant for those machines where software is found to be installed which typically resides on servers: databases and other middleware are examples. We have seen many instances of this. In most cases customer declarations that these are either installed in error or are used for development purposes are accepted. These declarations might well have not held up under more in-depth investigation. It's likely that these declarations are assumptions on the customers' part as well. Licensing decisions should be grounded in factual evidence as far as practicable.

Customers

For customers this provides just one more example of how difficult it is to reconcile the practical considerations of deploying software with the licensing rules underpinning it. Software asset management is an incredibly multidisciplinary field and no one person is likely to be able to master all the moving pieces. Default security settings which are never reviewed or even considered in a licensing context could have profound implications on the licensing of software, particularly if new circumstances such as technology, owners, leadership or commercial pressures, lead publishers or customers to revisit their terms for ambiguity and opportunities for hitherto unanticipated interpretations.

David Eastwood
Senior Managing Director
+44 (0) 203 727 1292
david.eastwood@fticonsulting.com

Gareth Coffey
Senior Director
+44 (0) 203 727 1714
gareth.coffey@fticonsulting.com