Third Intersessional Consultation of the AHC on Cybercrime

Presentation during the Panel "A concerted effort: the role of the private sector in the fight against the use of information and communications technologies for criminal purposes" by Will Hudson

Madame Chair and distinguished delegates, my name is Will Hudson, and I'm participating today on behalf of ICC United Kingdom. I'm a lawyer on Google's global data disclosure team, which is responsible for providing legal advice related to the disclosure of user data in response to law enforcement, administrative, and civil requests around the world. On behalf of both ICC UK and Google, thank you for the opportunity to speak with you today.

The private sector has a unique perspective on this historic effort given our role in the Internet's growth and operation. Cyber crime affects our users, can happen on our platforms, and transits our networks. At the same time, we have experience combating these abuses and responding to lawful government requests for user data from many jurisdictions around the world.

For similar reasons, members of civil society and the technical community are also well-positioned to share their perspectives given their years of experience working with victims and building secure systems more resilient to abuse.

The breadth and number of stakeholders invested in this process is an incredible opportunity to develop a Convention that builds off of decades of expert experiences confronting cyber crime from different perspectives. These experiences will make the final Convention a more effective instrument.

With that in mind, I'd like to quickly discuss three general observations drawn from Google's experience dealing with this issue in the private sector.

First, we all know that this is an incredibly complex area of law and policy. For that reason, it's important to ground the procedural elements of the Convention on *existing* international instruments and *existing* best practice. In order for the Convention to be its most effective, deviations from existing practice ought to be the exception rather than the norm, and only where there is a demonstrable added value to doing so.

Second, a successful Convention ought to minimise conflicts between laws that would ask providers to violate the law in one jurisdiction to comply with another's requirements.

Third, the protection of human rights and other fundamental freedoms ought to remain at the core of every part of the Convention, particularly its procedural elements. This will be the difference between an instrument that merely encourages the investigation of serious crime and one that promotes justice and the rule of law for everyone. Without it, many forms of cooperation will be more limited than would otherwise be the case.

Observation 1: Ground Procedures on Existing Instruments and Practice

Let me start with my first observation. If this Convention is to meaningfully counter serious cyber-dependent crime it must build off of the lessons we have all learned over the past two decades.

As you know, Google is a company highly focused on data-driven decisions.

Our Transparency Report data is clear: every year, we receive more requests for user data than the year before. Cross-border requests for data continue to account for a substantial portion of those requests. I don't expect this trend to change any time soon.

Google carefully reviews each of these requests to ensure it satisfies applicable laws. As you can imagine, given the number and variety of these requests, common procedural frameworks can help us more efficiently determine whether an individual request is valid and lawful — and respond to those that are valid — more rapidly.

To date, these common frameworks have included mutual legal assistance treaties between countries, universal instruments like UNTOC, and other approaches like the Budapest Convention on Cybercrime. More recently, the Second Additional Protocol to the Budapest Convention will enable state parties to make direct requests to foreign providers. Perhaps unsurprisingly, we've seen more and more countries express an interest in acceding to the Second Additional Protocol.

My point is not to endorse any particular instrument, or to say that they cannot be improved in one way or another. Rather, I'd just like to suggest that, by building off of an existing instrument's framework — particularly one that includes robust procedural protections and explicit human rights provisions — it will be simpler for both governments and private companies to more quickly adopt those requirements, the costs associated with doing so will be reduced, and the likelihood that requests will be favourably handled increases.

The alternative — where this Convention imposes requirements that are different from those contained in other instruments to which many states are already parties — would create confusion. This confusion, in turn, will produce delays, increase costs, and in some cases frustrate cooperation entirely.

For this reason, many States' written proposals have reproduced in their entirety articles from another instrument, or have noted that it's better to start from specific articles of those

instruments and to amend those articles in specific, narrowly tailored ways. We agree with this approach.

To that end, I would urge the Committee to incorporate by direct reference any procedural provisions in other widely-accepted international instruments, to deviate from those requirements in as narrow a way as possible, and to do so only when there's consensus that it's necessary.

Observation 2: Minimise Conflicts of Law

This brings me to my second point, which is that conflicts of law must be minimised to the maximum extent possible.

It's an obvious but important point that the law on some issues is simply different in jurisdictions around the world.

To give just a few examples, defamation isn't a criminal offence in the United States while it is in some other countries. Certain kinds of information must be retained only for a very limited time under some jurisdiction's privacy laws, whereas other countries would require that information to be retained for five years. There are countless other examples, but my overall point is that a company providing services to people around the world today must already contend with laws that have different and in some cases contradictory legal requirements relating to criminal offences and investigations.

For a global company, these differences lead to complex questions about whether it is appropriate to produce data, and under what circumstances, in response to requests that relate to those offences.

This Convention's procedural provisions shouldn't exacerbate these conflicts of law and put providers in an even more impossible position. Doing so will only frustrate our shared goal of countering serious cyber crime.

I'd like to suggest two specific ways the Convention could avoid these issues: first, focus on serious cyber-dependent crimes and second, include a dual criminality requirement.

The first is to focus the Convention on the detection, investigation, and prosecution of only *serious cyber-dependent* crimes. There is both more agreement among states over the elements of these offences, and a more pressing need to meaningfully reduce their occurrence. An international instrument is also more likely to prove effective dealing with these serious crimes.

The Convention could also avoid many conflict of laws issues by including a dual criminality requirement in its procedural provisions. This would require the crime under investigation to be the same or substantially similar in all relevant jurisdictions — a requirement that would make it

simpler for companies and governments to evaluate and respond to requests more quickly and effectively.

Observation 3: Protect Human Rights and Other Fundamental Freedoms

This brings me to my third and final observation, which is that the procedural provisions that are at the Convention's heart must recognize and protect international human rights law, privacy, and other fundamental freedoms.

Simply put, the Convention must not, in the name of reducing cyber crime, undermine the freedoms that have made the Internet such a powerful vehicle for free expression, civic discourse, economic opportunity, and community-building around the world.

As I noted just a minute ago, one important way of doing this is to limit the Convention's substantive scope to serious crimes that are truly cyber-dependent, instead of what we might call "crimes that happened on a computer."

The procedural elements of the Convention are an equally important way of ensuring it protects and expands the rule of law.

For example, a bedrock principle of the law is that accused parties ought to have the ability to examine the evidence being brought against them and to challenge it.

To remain true to that principle, the Convention should explicitly prioritise the right of individuals to be notified when providers receive government requests for their data, and for those users and their providers to be able to challenge those requests under applicable law, particularly when disclosure would not negatively impact ongoing investigations or prosecutions.

For similar reasons, the Convention could promote greater understanding regarding the scope of government requests for digital evidence by encouraging the regular publication of transparency reports related to those requests.

Finally, procedures that would allow the bulk collection of data, or the collection of data on a real-time basis, would be particularly problematic.

At the outset, most jurisdictions prohibit the real-time interception of data except in extremely narrow circumstances that are carefully prescribed under national laws with significant penalties for noncompliance. In other words, any provision related to this issue will unquestionably raise serious conflict of law issues. Moreover, it's worth remembering that real-time collection is not always technically possible.

By contrast, a Convention focused on more practical, less controversial elements will have a real chance of achieving its goal of reducing serious cyber crime.

Conclusion

I'd like to conclude by thanking you for inviting me to speak alongside my distinguished co-panelists, and to encourage you to continue to seek out the voices of non-governmental experts on this important issue. This is an historic opportunity to reach a global consensus on a sustainable solution to counter the growing threats posed by serious cyber crimes.

I am confident that a Convention which builds off of existing agreements, minimises conflicts of law, and protects human rights is both within reach and will prove highly effective.

We look forward to the opportunity to continue to share our perspective alongside other stakeholders as this process continues.

Thank you.