INTERNATIONAL CRIMINAL COURT

Office of the Prosecutor

JOINT COMMENTS ON THE DRAFT POLICY ON CYBER ENABLED CRIMES UNDER THE ROME STATUTE

Submitted by

Derechos Digitales
Electronic Frontier Foundation

May 30th, 2025

TABLE OF CONTENT

ABOUT US

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. EFF's mission is to ensure that technology supports freedom, justice, and innovation for all people of the world.[1]

Derechos Digitales is an independent non-profit Latin American organization founded in 2005, whose mission is the defense, promotion, and development of fundamental rights in digital environments in Latin America. Derechos Digitales has ECOSOC status and has actively contributed to the U.N and different of its thematic rapporteurs regarding the impact of digital technologies on human rights. We've actively participated in global processes relevant to digital technologies such as the Global Digital Compact, the UN Convention against Cybercrime, the Open-Ended Working Group (OEWG), and other relevant instances.[2]

Introduction

The Electronic Frontier Foundation and Derechos Digitales respectfully submit the enclosed joint comments regarding the Draft Policy on Cyber Enabled Crimes Under the Rome Statute, which is open for public input until 30 May.

Overall, the draft policy makes a strong and positive contribution by affirming the ICC Office of the Prosecutor's commitment to investigating and prosecuting crimes under the Rome Statute when committed or facilitated through cyber means. It appropriately avoids redefining "cybercrime," focusing instead on "cyber-enabled crimes" strictly within the Court's jurisdiction and makes clear that it does not have jurisdiction over ordinary "cybercrimes" that are punishable under domestic law. This clarity helps safeguard against the overreach seen in abusive cybercrime laws across the world that conflict with international human rights standards.

[1] https://www.eff.org/
[2] https://derechosdigitales.org

Our detailed contributions are outlined in the attached document. In particular, we wish to draw your attention to the following key points:

- The need to more clearly affirm human rights standards in the drafting of certain paragraphs where the necessity to investigate core crimes under the Rome Statute may threaten or come into conflict with the protection of rights such as freedom of expression or online privacy.
- The importance of articulating and affirming critical safeguards for online freedom of expression and privacy in the context of the prosecution of the most serious crimes, including the protection of encryption and anonymity online, and the importance of adopting a clear stance in defense of their enforcement and protection.
- The need to recognize critical nuances regarding the architecture of the internet (decentralized, universal, open) and its actors (intermediaries that play a key role in the functioning of the network) in discussions about their potential role in the facilitation or commission, whether direct or indirect, of crimes under the Rome Statute.
- The need to advance guidelines for the collection, preservation, and securing of digital evidence, given the ephemeral, volatile, and fast-moving nature of online content, as well as to acknowledge that technical factors, such as algorithms, may affect the availability, visibility, dissemination, and accessibility of content that may support the OTP's evidentiary work.

We appreciate the Office of the Prosecutor's openness to receiving input on this important initiative, and we remain at your disposal for any further questions or clarifications regarding our submission. We hope the final policy further clarify how civil society can engage with and support the OTP in implementing this policy.

Executive Summary

Paragraph 1: Add at the end of paragraph 1, text that reads:

"In providing such support, the Office will ensure that it remains strictly confined to matters falling within the Court's subject-matter jurisdiction, refraining from participation in investigations or prosecutions of ordinary cybercrimes under domestic law, and that all cooperation and capacity-building activities uphold internationally recognized human rights standards, in line with article 21(3) of the Statute."

Rationale: The text clarifies that OTP should avoid mission creeping into ordinary cybercrime. The text also explicitly ties all cooperation to Article 21(3) requirements, preventing endorsement or assistance of abusive practices. Placing it in Paragraph 1 sets the tone for the entire policy, ensuring consistent interpretation throughout, for example, see also paragraphs 4, 12, 29, and 107.

Paragraph 3(e): Building on the Draft Policy's call for enhanced cooperation with national authorities, the OTP should also urge States to reinforce transparency and oversight safeguards around criminal procedural measures and international cooperation, including joint investigations, that may generate ICC-relevant evidence.

Addressing New Technologies (Paragraphs 9-13)

Paragraph 9: Text to add at the end of Paragraph 9:

"Consistent with article 21(3) of the Statute, and recalling Human Rights Council resolutions 20/8 (2012)[3] and 32/13 (2016)[4] as well as UN General Assembly resolution 68/167 (2013),[5] all of which affirm that 'the same rights that people have offline must also be protected online,' the Office therefore reaffirms that every international human rights treaty binding on a State applies with full force to conduct online."

Rationale: The draft contextual anchoring in existing debates (Tallinn Manual, UN OEWG, Cybercrime Treaties) is valuable, but a direct reaffirmation that all human rights treaties apply online would solidify the normative baseline.

Paragraph 10: We welcome both the observation that existing crimes under the Rome Statute can be committed by cyber means, and the OTP's reiteration that its authority to prosecute these crimes—and their definition—derives from existing Rome Statute language and principles, in accordance with the *nullum crimen sine lege* Principle, and its foreseeability requirement.

Paragraph 12: States' "cybercrime" laws and corresponding cross-border cooperation under "cybercrime" treaties have often been overbroad and have targeted activities that ought to be protected prudentially and as a matter of international human rights law and standards, including good-faith computer security research and political dissent.[6] When pursuing collaborations with states in accordance with domestic cybercrime legislation, the OTP should be mindful of the need to remain focused on activity that can constitute a crime under the Rome Statute. The OTP should also be mindful of not appearing to lend its legitimacy to domestic investigations of matters far afield from such crimes. We recommend restating that cooperation and capacity-building will stay

[3] Resolution adopted by the Human Rights Council, A/HRC/RES/20/8. Available at: https://www.right-docs.org/doc/a-hrc-res-20-8/

[4] Resolution adopted by the Human Rights Council on 18 July 2016, A/HRC/RES/32/13. Available at: https://documents.un.org/doc/undoc/gen/g16/156/90/pdf/g1615690.pdf

[5] Resolution adopted by the General Assembly on 18 December 2013, A/RES/68/167. Available at: https://digitallibrary.un.org/record/764407/files/A_RES_68_167-EN.pdf

[6] Abusive cybercrime laws have often been misused to target online speech and political activity. Even laws targeting core cybercrime issues, such as access without authorization, have sometimes suffered from defects including the lack of a mens rea requirement and lack of protection for good-faith vulnerability research and penetration testing. Overbroad concepts of unauthorized access have led to criminal prosecutions of individuals for violating private terms of service.

strictly within the Rome Statute's mandate, and that any work with national cybercrime units on ordinary cybercrime offences such as computer access without authorization must include safeguards such as those outlined in the Council of Europe Budapest Convention explanatory memorandum,[7] and in a letter by 124 security researchers submitted in the context of the UN Cybercrime Treaty negotiation process to protect good faith security research and responsible vulnerability disclosure.[8]

History and Methods (Paragraphs 17-19)

Paragraph 19: We appreciate the open call for consultation, but urge additional targeted outreach, through regional hearings/meetings or online portals, to victims, diaspora communities, and NGOs in the Global South who disproportionately face cyber-facilitated persecution, as well as to researchers who focus on these phenomena.

Key terms and concepts (Paragraphs 20-29)

Paragraph 20: Add at the end of paragraph 20: "In the investigation and prosecution of crimes under the Rome Statute, 'cyber" encompasses not only the damaging or disabling of ICT systems *as a direct method of committing a crime*, but also the use of such systems to *prepare for, facilitate, or target* crimes, for example, by harvesting data to identify, locate, or track victims."

Rationale: This paragraph is consistent with paragraphs 26 and 27 which note that cyber means for committing international crimes do not have to violate domestic law and do not have to be a form of cyberattack.

Paragraph 29: In collaborating to "pool[] capabilities, techniques, skills, and procedures" on investigations, the OTP and ICC must be careful not to become complicit in national authorities' human rights abuses linked to "cybercrime" investigations, and must adopt safeguards related to the scope and purposes of such cooperation, to ensure that expertise provided by ICC to states is not abused, and that any technical assistance or expertise it provides is not misused to persecute civil society or suppress legitimate dissent.

Proposed redraft: Conduct criminalized under ordinary cyber-crime laws, such as illegal access or system interference, can also prepare, facilitate, or conceal Rome-Statute crimes; for example, assessing without authorization a hospital network may be the first step toward a war-crime attack. Accordingly, the Court and the Office may therefore sometimes share common investigative interests and pool technical capabilities with

[7] Council of Europe (November 23, 2001). Explanatory Report to the Convention on Cybercrime. Available at: https://rm.coe.int/16800cce5b

[8] Gullo, F. (February 7, 2024). Protect Good Faith Security Research Globally in Proposed UN Cybercrime Treaty, EFF. Available at: https://www.eff.org/deeplinks/2024/02/protect-good-faith-security-research-globally-proposed-un-cybercrime-treaty

national authorities. Any such engagement shall be subject to the five cumulative safeguards:

1. Cooperation must be strictly necessary and materially advance an ICC investigation or prosecution under the Rome Statute;
2. Assistance must be limited in time, scope, and data volume, consistent with the principles of legality, necessity, legitimate aim, and proportionality;
3. Measures must not criminalize or chill good faith security researchers, investigative journalists and whistleblowers;
4. Require national authorities to terminate cooperation where there is a credible risk that ICC expertise can be used to persecute civil society, suppress lawful dissent, or otherwise facilitate human rights abuses or transnational repression;
5. Require national authorities executing any OTP request for the collection, search, seizure, or transmission of digital evidence shall do so only through measures that are lawful, necessary, and proportionate and that fully comply with applicable international human rights standards, as required by article 21(3) of the Rome Statute.

Rationale: Across Latin America, broadly worded cyber-crime laws are routinely invoked to jail journalists, LGBTQ+ advocates, and political opponents for "illegal access" or "system interference".[9] The Inter American Commission on Human Rights has criticized such misuse in El Salvador, Cuba, Venezuela, and Nicaragua, yet the statutes remain in force. By linking any ICC cooperation to a material-advancement test and by requiring safeguards protections for good faith security researchers, journalists and whistleblowers, the revised paragraph ensures the Court can still obtain essential digital evidence without lending technical legitimacy to repressive cyber-crime regimes.

Tying ICC cooperation to a material advancement test, narrow time, and scope limits, and explicit protections for researchers, journalists, and whistle-blowers enables the Court to obtain critical digital evidence for Rome Statute prosecutions while withholding its expertise from investigations that seek to persecute human rights defenders and activists. These safeguards operationalize article 21(3)'s human-rights requirement and ensure the OTP cannot be co-opted to legitimize or facilitate domestic cyber-crime regimes that persecute civil society, activists, judges, and journalists.

[9] One of the most visible recent cases of the abusive use of cybercrime laws to criminalize experts is that of Swedish software developer, programmer, and activist Ola Bini, who has been prosecuted in Ecuador for over four years without solid evidence, in a politically motivated criminal trial. The State has accused Ola Bini of allegedly committing the crime of illegal access to a computer system. Hundreds of human rights organizations observing the case have spoken out against this type of criminalization, which sets a negative precedent for the defense of digital rights in Latin America. See also: Derechos Digitales (April 22, 2025). Debe ratificarse la inocencia de Ola Bini. Available at: https://www.derechosdigitales.org/25113/debe-ratificarse-la-inocencia-de-ola-bini/

Applicable Law and Jurisdiction (Paragraphs 28-44)

Paragraph 32. We recommend including an explicit reference to the right of women and girls –in all their diversity- to live free from violence, both online and offline, as a relevant human right in the application of the OTP's policy on the prosecution of cyber-enabled crimes under the Rome Statute.

Paragraph 42: While the draft helpfully rejects jurisdiction based solely on data packets that "simply transit" a State Party's servers, the operative territoriality[10]test remains with: "Consistent with Rule 9(2) of the Tallinn Manual 2.0, the Office will regard cyber-infrastructure located on a State Party's territory as a basis for territorial jurisdiction only where that infrastructure constitutes an integral facet of the alleged crime, thereby excluding de minimis or purely transitory connections.[11]

For example, if a spyware company builds a data exfiltration tool targeted toward a specific vulnerability in a mobile operating system, and chooses to, or necessarily must, deliver that malware through servers known to be located in a State Party, that use of the State Party located servers is an "integral facet" of the alleged crime that would establish jurisdiction.

The same logic applies once the implant is running. If the spyware exfiltrates data from the victim's device (or otherwise surveils the victim) while the device is physically in a State Party's territory, that device-based exfiltration or monitoring becomes an "integral facet" of the alleged crime, so the location of the victim's device provides independent grounds for jurisdiction.

Paragraph 40: We've listened to the OTP's position in recalling that, when it is not possible to clearly establish the element of territorial jurisdiction, the ICC's jurisdiction may, as a residual measure, be exercised on the basis of the nationality of those involved in the commission of crimes under the Rome Statute.

We have no concerns with using nationality jurisdiction when the identity of the perpetrator (defendant) in a consenting State is known. However, we know that it is often not technically nor legally possible to clearly establish the location, the identity, and subsequent nationality of perpetrators who used digital technologies to commit crimes. We do not want the OTP to use this unfortunate fact as an excuse to encourage

11 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Rule 9(2), p. 55

States to adopt legislative measures that undermine anonymity and encryption, or eliminate them altogether, as these online protections serve the average internet user.[12]

Nevertheless, the policy brief does not specifically address how the OTP intends to tackle these technical challenges–challenges that States themselves are already confronting and which the OTP will inevitably need to face as well, which leads us to ask: Does the OTP have a position on this issue, particularly in the context of global discussions that, under the banner of fighting cybercrime, seek to undermine safeguards such as encryption and online anonymity for the sake of criminal prosecution?

We recommend that OTP's consider the various reports from the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, which have affirmed the value of encryption and anonymity as technical tools that enable the exercise of the right to freedom of expression and privacy (A/HRC/23/40 and Corr.1). Any limitations on the protections provided by encryption and anonymity must meet the tripartite test: legality, legitimacy, and must pass the test of necessity and proportionality (A/HRC/29/32).

As recognized by the Rapporteur (A/HRC/29/32), States often invoke the need to weaken these encryption safeguards (through, for example, backdoors) and anonymity (through, for example, internet service provider liability regimes) in order to advance efforts to combat terrorism and other crimes that threaten national security. However, such measures are frequently justified with insufficient reasoning and without consideration of alternative mechanisms that are equally effective in fighting crime. The Rapporteur has emphasized that guarantees which are critical to resisting state surveillance should not be sacrificed, as they also serve as protective mechanisms for groups in situations of particular vulnerability (such as political opponents, dissidents, human rights defenders among others).

Genocide (Paragraphs 47-50)

Paragraphs 47 to 50: In the context of the policy brief, we consider it extremely relevant to include examples such as those presented in these paragraphs. Several of the cases cited throughout the document specifically refer to situations in which a social media post may be regarded as facilitating, or even directly or indirectly constituting, the commission of a crime under the Rome Statute.

In this regard, we wish to highlight concerns that some online platforms disproportionally amplify emotive, violent extremists or otherwise polarizing content

[12] Levy, S. (July 21, 2023). Almost 50 years into the crypto wars, encryption's opponents are still wrong. WIRED. Available at: https://www.wired.com/story/plaintext-50-years-into-the-crypto-wars-encryptions-opponents-are-still-wrong/; Yen, A. (February 25, 2025). The UK government's war on encryption is a global threat. PROTON. Available at: https://proton.me/blog/apple-ends-adp-in-uk

with the goal of maximizing user engagement, and thereby online ad revenues. Such amplification may take place due to the design of platforms' recommender systems. It may also occur to the abuse or 'gaming' of recommender systems or other platform features by coordinated actors(which may operate at national or transnational levels).In light of this, does the OTP have a position on the role played by recommender systems in amplifying, curating or giving visibility to content that publicly and directly incites the commission of genocide, which might not have had the same reach without such amplification? Furthermore, could the deliberate design of recommender systems that actively promote such messages be interpreted as a causal contribution to the commission of the crime, in line with the statements below regarding paragraph 50?

Paragraph 50 notes that direct and public incitement to genocide is prosecutable under Article 25(3)(e) even when no genocide occurs. Still, under Article 21(3), the Prosecutor must apply that provision consistently with ICCPR Article 19. International jurisprudence (HRC General Comment 34, the Rabat Plan of Action, ICTR Nahimana Appeals Judgment) requires a context–likelihood–intent test: speech may be criminalized only when, in its full social setting, it was reasonably likely to trigger imminent genocidal violence and was uttered with the specific intent to destroy a protected group. Rabat expresses this through six factors (speaker, intent, content, context, likelihood, and form), which together provide a structured free-expression safeguard.

The draft policy notes the potential for commission of "the offence of direct and public incitement to genocide, as provided for in article 25(3)(e) of the Statute (Paragraph 50). Footnote 27 promises a gravity assessment (further detailed in Paragraphs 34 and 94-97). Both the Council of Advisers and the OTP correctly treat incitement as an inchoate crime that does not require a completed genocide in order to incur international criminal liability. Yet, to protect freedom of expression, the impugned speech must be of a kind that could reasonably be expected to incite genocidal action; mere statements of opinion, even harsh political views on an armed conflict, fall outside Article 25(3)(e) unless the Rabat criteria are met. We interpret Paragraph 50 as *not* implicating intermediary liability, and as only relating to the actual speakers online.

Recommendation: (i) Embed the Rabat six-factor test within its gravity assessment, expressly treating the "plausible risk of imminent harm" as a speech-protective threshold; and (ii) make clear that prosecution will not proceed where the alleged incitement is detached from a context in which genocidal acts could reasonably be foreseen.

These additions would align Paragraph 50 with Article 21(3) and international free-expression norms while preserving the Court's ability to act against genuinely dangerous cyber-incitement.

Proposed redraft:

"50. A more likely scenario for the standalone prosecution of cyber operators arises from the offence of direct and public incitement to genocide, as provided for in article 25(3)(e) of the Statute. This is an inchoate offence that does not itself require genocide actually to have been committed or, if it was committed, for the act of direct and public incitement to have causally contributed to it. Consistent with article 21(3) and international freedom-of-expression standards (ICCPR article 19, HRC General Comment 34, and the Rabat Plan of Action), the Office will apply a "context–likelihood–intent" analysis, assessing the speaker, intent, content, context, likelihood, and form of the communication, to ensure that only speech reasonably likely, in its circumstances, to prompt imminent genocidal violence is pursued; mere expressions of political opinion that do not meet this threshold fall outside article 25(3)(e). In the view of the Office, there is no doubt that direct and public incitement of genocide can be committed by cyber means, for example, through postings on social-media platforms. When made with the requisite intent and meeting the contextual threshold set out above, such postings could satisfy the relevant actus reus requirements and be prosecuted as such, having regard to the context in which they were made, and provided that the statement(s) concerned were sufficiently direct."

War Crimes (Paragraphs 61 to 73)

The online world and people's personal data are real and are essential parts of people's lives, social, cultural, and family relationships—whether one can point to concrete physical or offline harm from disrupting a specific ICT system, or not. Civilians' ability to communicate with one another, to track their schedules, obligations, personal histories, to coordinate and plan with one another electronically, and to discuss and deliberate digitally, is essential on every level. These realities should be recognized by international law in confirming that an attack on the functionality of an ICT system is an "attack" (paragraph 69) and that data is a "civilian object" (paragraph 70).

First, it is increasingly unavoidable that disruption of ICT systems will lead to severe offline consequences for civilians. ICT systems are heavily enmeshed in the provision of all essential infrastructure and essential services, from medical care to power and water provision to transportation to the food supply.

Second, civilians have a fundamental reliance on ICT systems to lead and organize their day-to-day personal, social, and family lives. This reliance is heightened during a military conflict where civilians may need to coordinate to improve the resilience of their local communities, learn about the availability of resources and emergency services, maintain family ties, check on others' safety, and communicate with others outside of a war zone. They may need to obtain and share details that affect their safety

and decision making amidst the conflict. They also need to be able to record and document their own experiences, increasingly by means of digital technology. In many cases, access to ICTs can be a matter of life and death, enabling civilians to request or provide first aid, locate emergency medical services, and coordinate the delivery of humanitarian aid. Digital tools also empower individuals to document their experiences, gather and share evidence of potential violations, and make informed decisions under rapidly changing and dangerous conditions. Disrupting or denying civilian access to these systems may not only violate human rights but may also undermine civilian protection, humanitarian response efforts, and post-conflict accountability.

The OTP's could underscore the value that would result from clearer protections of ICT functionality and data in applying the Geneva Convention by stressing the centrality of computing and communications throughout modern civilian life.

Offences Against the Administration of Justice (Paragraphs 78-81)

Paragraph 81. As acknowledged by the OTP's, the administration of justice of the ICC can be threatened by offenses facilitated through digital means. Based on the information provided regarding the cyberattack suffered by the Court in 2013, we recommend that both the OTP's and the ICC implement an obligation to notify individuals affected by digital security breaches that compromise the confidentiality, integrity, and availability of information that could be weaponized against them—particularly when such attacks involve the leak of personal data. In such cases, data subjects may need to take measures to protect both their personal information and their physical or personal safety.

The notification obligation has been adopted by various data protection laws, including the European Union's General Data Protection Regulation (GDPR), Article 33. It has also been recognized as a good practice by the OECD in its *"Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,"* specifically in point 15, section C.

Facilitating Rome Statute Crimes by Cyber Means (Paragraphs 82-87)

Paragraph 83 already indicates that the Office will look at an individual's function and mental element before treating that person as a facilitator. We simply encourage one extra sentence to ensure this point is unmistakable. In today's layered ecosystem, actors range from backbone engineers who pass packets, through cloud-hosting teams that store data automatically, to product leads who fine tune recommendation engines, and on to suppliers of bespoke spyware. The differences between those roles are significant. In particular, merely knowing that third-party speech sits on one's servers is not the same as providing a customized tool that can be used to target victims. We therefore suggest that the Policy explicitly note that different technical contributions may warrant different legal analyses, so that routine hosting of user content is not automatically

conflated with more purposive forms of assistance. As noted by paragraph 125 of the explanatory report to the Budapest Convention on Cybercrime, "a service provider does not incur liability by virtue of the fact that a crime was committed on its system by a customer, user or other third person...."

Improper Incentives to Remove Content Can Destroy Evidence

Imposing criminal liability on routine platform operations would drive companies to "over-comply". They would err on the side of mass deletion, expand algorithmic filters, and adopt invasive monitoring simply to minimize remote litigation risk. That defensive stance has a predictable knock-on effect, the erasure of evidence that future ICC or national prosecutors may need to bring cases.

When YouTube tightened its machine-learning extremism filter in 2017-18, the algorithm swept away more than 206,000 videos from the Syria conflict, among them at least 381 clips that independent researchers had already authenticated as showing air-strikes on hospitals. Those files, originally posted by victims, rescuers, and local journalists, vanished because the system mistook human rights evidence for terrorist propaganda. With them went timestamps, geolocation data, and visual proof that international and national prosecutors, including, potentially, the ICC, may one day need to establish individual responsibility for war crime attacks on medical facilities.

Recommendation: The OTP should avoid incentivizing online platforms to destroy online evidence of crimes out of fear of being held liable for their content by encouraging online platforms to apply exemptions for content that is educational, documentary, artistic or news-worthy. Without such policies, automated moderation algorithms that cannot understand the context or significance of a particular material may lead to the over removal of legal content. The draft policy also refers to a desire to achieve "non-prosecutorial outcomes which may serve to deter or to disrupt crimes under the Statute, or to mitigate the harm caused [...] such as [in crimes] based on the dissemination of material calling for the commission of genocide, crimes against humanity, war crimes, or aggression" (paragraph 119). This appears to be expressing a general hope that Internet intermediaries (or, perhaps, content creators) might be induced to remove access to such content. In addition to caution about the free expression impacts of these goals, we urge the OTP to be cautious about the risk of destroying important evidence and documentation of crimes, whether it is shared by perpetrators, victims, or bystanders.

Procedural Safeguards for Digital Evidence, Cooperation and Joint Investigations (Paragraphs 114, 117-121)

The draft policy affirms that the OTP will use its investigative powers and seek cooperation under national laws per Article 93 of the Rome Statute. It may also request voluntary cooperation from private entities within domestic legal bounds as per paragraph 125. Because investigations of individuals—whether conducted by states, the OTP, or in cooperation between them—involve access to sensitive personal data, they inherently constitute an interference with individuals' private lives. Therefore, the used of investigatory measures and the collection, monitoring, access, storing, sharing and use of personal data inherently implicates internationally protected human rights, and article 21(3) of the Rome Statute obliges the Office to act "consistent with internationally recognized human rights." The Court's existing rules of evidence and procedure provide relatively little guidance about the proper protection of suspects' (and others') rights with respect to intrusive investigative measures, but international human rights law imposes various requirements in this regard. Currently, most safeguards are left to the "applicable legal obligations" of cooperating States, which may vary in how comprehensively they track international norms.[13]

The OTP's intention to enhance its capacity in digital evidence collection and conducting digital evidence is indeed broadly appropriate in keeping with the ever-greater role of such evidence in national and international criminal cases. However, it also provides an opportunity to be clearer about privacy and data protection safeguards that must apply to the exercise of intrusive powers. In the digital realm, safeguards around the use of these powers rest on three mutually reinforcing principles: legality, legitimate aim, necessity, and proportionality, prior judicial authorization, notification to users, oversight. There is already a substantial amount of international jurisprudence about these principles in the context of digital surveillance and similar measures. We and others have also written extensively about human rights safeguards applicable to surveillance measures.

As the Rome Statute expressly requires respect for internationally recognized human rights, and as the OTP expects to broaden its access to intrusive investigatory powers whose use affects these rights, we encourage the OTP to become familiar with jurisprudence in this area and be clearer about what safeguards will govern its use of investigatory powers, and require national authorities to ensure that any steps taken to collect or share digital evidence comply with international human rights law and standards. Deferring entirely to national law is not sufficient in this context because—as international jurisprudence has also made clear—many existing national legal regimes

[13] Privacy Interantional, PI's Guide to International Law and Surveillance, https://privacyinternational.org/report/5403/pis-guide-international-law-and-surveillance; Electronic Frontier Foundation (2013). Necessary and Proportionate, on the application of human rights to communications surveillance. Available at: https://necessaryandproportionate.org/

governing criminal procedural measures and international cooperation do not fully meet international standards[14]. Additionally, the policy should explicitly state that the OTP will not rely on evidence obtained through rights violating methods, such as mass surveillance or breaking encryption, and will not request personal data from private entities without prior judicial authorization. They must also require national authorities to ensure effective oversight and user notification—before surveillance where possible, or afterward once it no longer endangers investigations, including in real-time interception cases—to allow individuals to access, challenge, or seek redress for unlawful surveillance.

Joint Investigations & Cross-Border Cooperation (Paragraphs 130-134)

The Draft Policy's embrace of joint investigations can improve efficiency yet experience under the Budapest Convention Second Additional Protocol shows how JIT agreements can sidestep essential safeguards. We therefore urge the OTP to:

- Mandate a human-rights clause stipulating that JITs may not derogate from the Rome Statute's art. 21(3) obligation to apply "internationally recognized human rights."
- Limit duration and scope: agreements should be time-bound and investigation-specific.
- Prevent forum shopping: require that where multiple jurisdictions can execute an equivalent investigative measure, the path affording *greater* rights protection must be chosen.
- Ensure independent oversight and public reporting on the frequency, scope, and human rights impact of JIT activities.

Public Oversight and Investigative Powers

The Policy should establish an independent oversight mechanism within the Court to ensure transparency and accountability in any investigative power and international cooperation undertaken or requested by the OTP. This independent body must have full access to all relevant information, including classified material, so it can verify legality, necessity, and proportionality; assess whether published transparency statistics are complete and accurate; issue periodic public reports; and make determinations on compliance with international human rights standards. The mechanism would operate in addition to, not in place of, any existing oversight by other branches of the Court.

[14] Privacy International (March, 2024). Guide to International Law and Surveillance. Available at: https://privacyinternational.org/sites/default/files/2024-09/2024%20GILS%20version%204.0.pdf

Additional Concerns: The ICC, U.S Coercive Measures and its Relationship with Tech companies

At his point, we acknowledge that the International Criminal Court (ICC) as well as the Office of the Prosecutor have recently been subjected to coercive measures, particularly promoted by the United States government, aimed at hindering their work in investigating the commission of crimes against humanity in Palestine[15]. We also recognize the risks associated with carrying out the mandate of the ICC and the Prosecutor's Office, which have recently been affected by a technological blackout because of U.S. sanctions, through the instrumentalization of services provided by Microsoft to both institutions[16].

Given the risks that may arise from the publication of this policy paper—which directly addresses discussions related to the duties of transnational technology companies based in the United States, especially in light of the latest measure issued by that country's government threatening to revoke the visas of any public officials who issue decisions[17] of any kind that impose content moderation measures on U.S. companies—we call on the Office of the Prosecutor to proceed with the publication of this policy paper while maintaining and ensuring, as it has done so far, its autonomy and technical independence so that these threats do not influence or affect the content of the document in question.

[15] Human Rights Watch (December 2, 2024). ICC: Member States Should Act to Protect Justice. Available at: https://www.hrw.org/news/2024/12/02/icc-member-states-should-act-protect-justice

[16] Krempl, S. (May 19, 2025). Criminal Court: Microsoft's email block a wake-up call for digital sovereignty. Available at: https://www.heise.de/en/news/Criminal-Court-Microsoft-s-email-block-a-wake-up-call-for-digital-sovereignty-10387383.html

[17] Secretary of State, U.S Department of State (May 28, 2025). Announcement of a Visa Restriction Policy Targeting Foreign Nationals Who Censor Americans. Available at: https://www.state.gov/announcement-of-a-visa-restriction-policy-targeting-foreign-nationals-who-censor-americans/