The State of Communication Privacy Law in Panama

Katitza Rodriguez,
International Rights Director
(EFF)

Veridiana Alimonti,
Latin American Senior Policy
Analyst (EFF)

In collaboration with:

Abdías Zambrano
(IPANDETEC)

Authors: Katitza Rodriguez and Veridiana Alimonti
Collaborators: Abdías Zambrano (IPANDETEC)

EFF's Associate Director of Research, Gennie Gebhart edited this report. EFF's Engineering and Design Project Manager, Kim Carlson, along with EFF's Art Director, Hugh D' Andrade and EFF's Education & Design Lead, Soraya Okuda designed and formatted this report. EFF's engineers, Syd Young, Artemis Schatzkin, and Will Greenberg developed the revamped version of the Necessary & Proportionate website.

EFF would like to thank Luiza Rehder do Amaral, EFF Tecs-USP Fellow (2019) for her research and contributions to this report.

A publication of the Electronic Frontier Foundation, 2020.

JUNE 2020

INTRODUCTION

This report provides condensed information on the rules for government access to communication data in criminal investigations in Panama. It offers brief and straightforward answers on a set of relevant questions regarding when and under which conditions law enforcement authorities can gain access to users' communications data in criminal investigations as well as an overview of transparency obligations and practices.

This FAQ is intended for non-lawyers who want some general information about the legal framework for government access to data, but is not legal or technical advice.

The legal questions raised by this FAQ can be complex and the legal risks in any case will depend on the particular facts and on legal doctrines not necessarily mentioned here. This FAQ is meant to familiarize you with some of the principles involved, so that you can have a more effective discussion if and when you engage an attorney to help you with your particular circumstance.

DATA PROTECTION OVERVIEW

1. Is there a data protection law?

Panama's data protection law was approved in 2019 and will come into force in March 2021.[1]

2. Is there a data protection authority?

The country's data protection law, in force as of March 2021, appointed as its oversight body the existing National Authority for Transparency and Access to Information *(Autoridad Nacional de Transparencia y Acceso a la Información - ANTAI)*.[2] ANTAI is an independent authority, having functional and administrative autonomy to perform its functions.[3] The data protection law has created a multistakeholder Personal Data Protection Council to advise ANTAI in its functions regarding data protection.[4]

3. Does the data protection law apply to law enforcement activities?

The data protection law does not apply to the processing of personal data for national security purposes or for the prevention, investigation, detection, or prosecution of criminal offenses or execution of criminal penalties.[5]

4. What are the criteria, if any, for the transfer of personal data to third countries under their data protection law?

Article 33 of the data protection law sets out the general conditions for a data transfer to be lawful. Additionally, article 5 lays down that the transfer of personal data that are confidential, sensitive, or restricted in any way is allowed when the company responsible for storing or processing such data, and/or the destination country, have standards of protection comparable to those set in the data protection law. It is also allowed if the entity transferring the data takes all the necessary steps to protect them. Exceptions to these requirements are: (1) when the data subject has given his/her consent for the transfer; (2) when the transfer is necessary for the conclusion or

[1] Article 47, Data Protection Law - Law 81/2019 (*Ley 81 de 26 de marzo de 2019 - Sobre Protección de Datos Personales*), https://www.antai.gob.pa/wp-content/uploads/2019/04/Ley-81-de-2019-Proteccion-de-Datos-Personales.pdf (Spanish)
[2] See Article 7, para 3; Article 17, para 2; Article 18, Article 31, Article 16, and Article 45, Data Protection Law.
[3] Article 1, Law 33/2013 (*Ley 33 de 25 de abril de 2013 -- Que crea la Autoridad Nacional de Transparencia y Acceso a la Información*), https://www.antai.gob.pa/wp-content/uploads/2015/04/ley33-25-abril-2013.pdf (Spanish)
[4] Articles 34 and 35, Data Protection Law, https://www.antai.gob.pa/wp-content/uploads/2019/04/Ley-81-de-2019-Proteccion-de-Datos-Personales.pdf (Spanish)
[5] Article 3, para 2 and 3, Data Protection Law.

execution of a contract concluded or to be concluded by the interested party in his/her interest; (3) bank, monetary, or stock market related transfers; and (4) when such transfer is required for complying with international treaties ratified by Panama. Regardless, the transfer must follow proper security standards and protocols in order to ensure the level of protection as laid down by the data protection law and existing rules and certifications.[6]

[6] Article 5, para 3 and 4, Data Protection Law.

COMMUNICATIONS PRIVACY LAW

5. What's the legal authorization needed to access communications data?

Interception of communication

Panama's Constitution states that private communications are inviolable and cannot be intercepted or recorded without an order by a judicial authority. Failing to comply with this provision prevents the use of the results as evidence and may also incur criminal responsibilities.[7] Reaffirming this safeguard, the country's Supreme Court of Justice has ruled that "judicial authority" refers only to judges, thereby not including the Public Prosecutor's Office.[8] The Criminal Procedure Code stipulates the need of a judicial order (*juez de garantías*), following a prosecutor's request, to authorize the interception of conversations and digital communications. The interception period must not exceed 20 days, but can be extended at the prosecutor's reasoned request.[9] The same applies to investigations against organized crime. In this case, the interception authorization can be up to three months, eligible for extension for the same period provided there is a prior judicial order and the interception is conducted for the specific purposes of the investigation.[10]

Access to the content of communications and metadata

Referring to Article 29 of Panama's Constitution, the Supreme Court of Justice has stated that the concept of correspondence exceeds the simple epistolary exchange between two or more people, covering all individuals' private documents.[11] According to the Criminal Procedure Code, the seizure of correspondence and other private documents requires a previous judicial order.[12] However, access to stored data in seized electronic devices is subject only to subsequent judicial review within no more than 10 days.[13] The accused

[7] Article 29, para 3 and 4, Panama's Constitution (*Constitución Política de la República de Panamá*), https://vlex.com.pa/vid/constitucion-politica-panama-40575284?_ga=2.254341262.721673092.1580504836-202611048.1580504836 (Spanish)
[8] Ruling of the Plenary of the Supreme Court of Justice on July 17th, 2007, https://vlex.com.pa/vid/accion-inconstitucionalidad-suprema-pleno-31663428?_ga=2.7846196.721673092.1580504836-202611048.1580504836 (Spanish).
[9] Article 311, Criminal Procedure Code (*Ley 63 de 28 de agosto de 2008 - Que adopta el Código Procesal Penal*), https://vlex.com.pa/vid/codigo-procesal-penal-42484053?_ga=2.6352948.721673092.1580504836-202611048.1580504836 (Spanish). The Criminal Procedure Code had some of its articles amended by Law 121/2013. The legal references in this report will highlight the new wording when mentioning an amended article.
[10] Article 24, Law 121/2013 (*Ley 121 de 31 de diciembre de 2013 - Que reforma el Código Penal, Judicial y Procesal Penal y adopta medidas contra las actividades relacionadas con el delito de delincuencia organizada)*, http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/95580/112588/F-86115861/PAN95580.pdf (Spanish)
[11] Ruling of the Plenary of the Supreme Court of Justice on July 17th, 2007, https://vlex.com.pa/vid/accion-inconstitucionalidad-suprema-pleno-31663428?_ga=2.7846196.721673092.1580504836-202611048.1580504836 (Spanish).
[12] See Article 29, para 1 and 3, Panama's Constitution, https://vlex.com.pa/vid/constitucion-politica-panama-40575284?_ga=2.254341262.721673092.1580504836-202611048.1580504836 (Spanish), Article 310, Criminal Procedure Code, https://vlex.com.pa/vid/codigo-procesal-penal-42484053?_ga=2.6352948.721673092.1580504836-202611048.1580504836 (Spanish)
[13] Article 314 and 317, Criminal Procedure Code.

and their defense will be notified to take part in the analysis of the data contained in the seized devices.[14] As per Law 121/2013, which addresses the investigation of organized crime, the seizure of correspondence, including electronic data, and other private documents follows the procedure described above for interception measures, requiring a previous judicial order.[15] In turn, access to stored data in seized devices not considered as "electronic correspondence" abides by article 314 of the Criminal Procedure Code, therefore subject to subsequent judicial review. For organized crime investigations, the deadline for such review is 60 days.[16]

With regards to traffic data, Law 51/2009 requires telephone and Internet service providers, including resellers and Internet cafés, to hand over to public prosecutors or the judicial authority any information contained in their systems that is required for the investigation and prosecution of crimes.[17] The prosecutor is allowed to file a direct, reasoned request, subject to subsequent judicial review.[18] The traffic data they are obligated to retain and make available include, among others, connection logs, call records, the type of services used (such as voice and multimedia messages), email accounts, and the location of mobile devices. For prepaid services, it also includes the date, time, and location of their activation.[19] The data retained in compliance with this law are deemed confidential information and can only be provided in accordance with Panama's legal framework.[20]

Access to subscriber data

The judicial authority or public prosecutors may also request access to subscriber data that telephone and Internet service providers, including Internet cafés and other similar facilities, have in their systems.[21] The prosecutor must file a reasoned request which is subject to subsequent judicial review.[22] According to Law 51/2009, subscriber data include name, address, copy of identity card or passport, and IMSI and IMEI numbers of users' devices. Names and addresses associated with email accounts provided by telecom companies are also included.[23]

Identification by IP addresses

Both the judicial authority and public prosecutors can request identification via IP addresses, following the regime applied to traffic and subscriber data.

[14] Article 314, paragraph 2, Criminal Procedure Code.
[15] Article 24, Law 121/2013, http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/95580/112588/F-86115861/PAN95580.pdf (Spanish)
[16] Article 317 of the Criminal Procedure Code, amended by article 47 of Law 121/2013, http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/95580/112588/F-86115861/PAN95580.pdf (Spanish).
[17] Article 11, Law 51/2009 (*Ley 51 de 18 de septiembre de 2009 - Que dicta normas para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones y adopta otras disposiciones)*, https://docs.panama.justia.com/federales/leyes/51-de-2009-sep-23-2009.pdf (Spanish).
[18] Article 12, Law 51/2009.
[19] Article 2, Law 51/2009.
[20] Article 10, Law 51/2009.
[21] Article 11, Law 51/2009.
[22] Article 12, Law 51/2009.
[23] Article 2, Law 51/2009.

Location data

The location of the mobile device and of the cell tower where a communication starts, or which registered the activation of a prepaid mobile service, can be requested by the judicial authority or directly by public prosecutors,[24] subject to subsequent judicial review.[25] The Criminal Procedure Code also stipulates that "satellite tracking" may be authorized by a judge (*juez de garantías*) at the prosecutor's request.[26] The judge must set a period up to 20 days, eligible for extension at the prosecutor's reasoned request. Within the scope of Law 121/2013, the prosecutor may order police agents to surveil and track individuals, groups, organizations, and objects of any nature, which can be carried out by any means, including electronic and technological ones.[27] The prosecutor's order is subject to subsequent judicial review within 60 days.[28]

6. What's the factual basis to access communications data?

Content and metadata

Panama's Constitution states that the access to correspondence and private documents must be carried out for specific purposes and following legal procedures. The Criminal Procedure Code and the laws on criminal organizations and data retention underscore access to communications data as part of a specific criminal investigation.[29] The Criminal Procedure Code also states the *exceptional nature* of communications intervention, which entails recording conversations, digital communications interception, "satellite tracking," and electronic surveillance.[30] Finally, telephone and Internet companies, or Internet cafes, are bound to hand over communications data when they are *required for* the investigation of crimes, or the detention and prosecution of persons directly or indirectly linked to the commission of such crimes.[31] The prosecutor's direct request for traffic data must be reasoned and follow the proportionality and exceptionality principles.[32]

[24] Article 2, (5), b and (6), Law 51/2009.
[25] Article 12, Law 51/2009.
[26] Article 311, Criminal Procedure Code, https://vlex.com.pa/vid/codigo-procesal-penal-42484053?_ga=2.6352948.721673092.1580504836-202611048.1580504836 (Spanish)
[27] Article 15, Law 121/2013, http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/95580/112588/F-86115861/PAN95580.pdf (Spanish)
[28] Article 16, Law 121/2013.
[29] Article 311, Criminal Procedure Code, https://vlex.com.pa/vid/codigo-procesal-penal-42484053?_ga=2.6352948.721673092.1580504836-202611048.1580504836 (Spanish); Article 24, Law 121/2013, http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/95580/112588/F-86115861/PAN95580.pdf (Spanish); and Article 12, Law 51/2009, https://docs.panama.justia.com/federales/leyes/51-de-2009-sep-23-2009.pdf (Spanish).
[30] Article 311, Criminal Procedure Code,
[31] Article 11, Law 51/2009, https://docs.panama.justia.com/federales/leyes/51-de-2009-sep-23-2009.pdf (Spanish).
[32] Article 12, Law 51/2009.

The measures authorized by Article 15 of the law on the investigation of criminal organizations, that could entail location tracking, also have to observe some legal requirements. Prosecutors can directly order them to police when there is a well-founded presumption that a crime is being committed or prepared. In addition, the purpose of the measures must consist of verifying facts, details, situations, links, or behaviors that are useful to such investigation.[33]

Subscriber data

Law 51/2009 lays down legal standards for accessing subscriber data, along with mandating their retention. According to Article 11, the data are to be provided for specific purposes set by law and must be necessary for the investigation of crimes or the detention and prosecution of persons directly or indirectly linked to the commission of such crimes.[34] As with traffic data, the prosecutor's direct request for subscriber information has to be reasoned and meet the proportionality and exceptionality principles.[35]

7. Which authorities have the legal capacity to request access to communications data?

In the context of a criminal investigation, the competent authorities to request access to communications data are public prosecutors and judges, following a prosecutor's request.[36]

8. Does the country have provisions about access to data in cases of emergency?

The Criminal Procedure Code allows the parties to request the judge for anticipated production of evidence in "urgent" cases, described as: (i) a measure considered as a definitive and irreproducible act due to its nature or the circumstances; (ii) statements likely not to be received during the trial due to an obstacle difficult to overcome; (iii) when the accused is a fugitive and the passage of time may hinder evidence preservation; and (iv) when the delay risks losing the evidence source.[37] The need of a prior judicial order for the seizure of correspondence and private documents may be lifted when this is required to avoid the commission of a crime, to rescue victims of

[33] Article 15, Law 121/2013, http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/95580/112588/F-86115861/PAN95580.pdf (Spanish)
[34] Article 11, Law 51/2009, https://docs.panama.justia.com/federales/leyes/51-de-2009-sep-23-2009.pdf (Spanish).
[35] Article 12, Law 51/2009.
[36] Article 311 and 314, Criminal Procedure Code, https://vlex.com.pa/vid/codigo-procesal-penal-42484053?_ga=2.6352948.721673092.1580504836-2026110481580504836 (Spanish); Article 24 and 25, Law 121/2013, http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/95580/112588/F-86115861/PAN95580.pdf (Spanish); and Article 11, Law 51/2009, https://docs.panama.justia.com/federales/leyes/51-de-2009-sep-23-2009.pdf (Spanish).
[37] Article 279, Criminal Procedure Code, https://vlex.com.pa/vid/codigo-procesal-penal-42484053?_ga=2.6352948.721673092.1580504836-2026110481580504836 (Spanish)

crimes or disasters, when the person is caught in the act of committing a crime, or there is a risk of evidence loss.[38] These cases are subject to subsequent judicial review (*juez de garantías*) within 48 hours. The judge will determine whether the seizure was justified regarding the prosecutor's reasons and evidence available at the time. If considered unjustified, the resulting evidence will be deemed unlawful and removed from the proceeding files.[39]

9. Is there any data retention mandate?

Law 51/2009 sets out rules for the retention, protection, and handover of telephone and Internet users' data for criminal investigation purposes. The law stipulates data retention obligations aiming at: (i) tracking and identifying the origin of a communication; (ii) identifying the recipient of a communication; (iii) establishing the time, date, and duration of a communication; (iv) identifying the type of communication; (v) identifying the communication device; (vi) identifying the location of the mobile device and the cell where a communication starts.[40] Article 2 of the law details the data relating to each category, covering users' name and address, copy of identity card or passport, IMSI and IMEI numbers of users' devices, and names and addresses associated with email accounts provided by telecom companies. As for traffic data, the law mentions connection logs, call records, forwarding phone numbers, the type of services used (such as voice and multimedia messages), email accounts, and the location of mobile devices, as well as the date, time, and location of prepaid mobile services' activation.

The retention obligation applies to telephone and Internet service providers, including resellers, Internet cafés, and other similar facilities.[41] The data must be retained for six months. A judicial order may extend the retention of certain data for up to the same period, taking into account the additional costs involved, as well as the relevance of such data to detention, investigation, and prosecution purposes.[42] Following a judge's or prosecutor's request, concessionaire companies are bound to provide the information in five business days when they relate to records within the six-month period. The deadline is longer—15 business days—when the request refers to records pertaining to the extended retention period.[43]

10. Are there any rules that authorize the use of malware?

There are currently no laws that explicitly authorize the use of malware.

[38] Article 310 combined with Article 298, Criminal Procedure Code. The same is applied for "electronic correspondence" in organized crime investigations as per article 24 of the Law 121/2013, http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/95580/112588/F-86115861/PAN95580.pdf (Spanish).
[39] Article 306, Criminal Procedure Code, https://vlex.com.pa/vid/codigo-procesal-penal-42484053?_ga=2.6352948.721673092.1580504836-202611048.1580504836 (Spanish)
[40] Article 2, Law 51/2009, https://docs.panama.justia.com/federales/leyes/51-de-2009-sep-23-2009.pdf (Spanish).
[41] Article 1, Law 51/2009.
[42] Article 6, Law n. 51/2009.
[43] Article 15, Law 51/2009.

11. Is there any law that compels companies to provide direct access to their internal servers for law enforcement purposes?

To the best of our knowledge, there is no legal provision authorizing this kind of access in criminal investigations.

12. Does the law compel companies to assist law enforcement agencies in their investigations?

The laws regarding the investigation of criminal organizations and the retention of communications data have explicit provisions requiring obliged parties to carry out the investigative measures or to provide the information requested in compliance with conditions set by law.[44] "The obliged parties" usually refers to telecommunication services providers, and requirements can be stricter to concessionaire companies. Law 51/2009 stipulates a specific deadline for them to hand over retained data in addition to the obligation to assign specialized staff for complying with the requests.[45] However, there is also a general provision on duty of assistance in the law on the investigation of criminal organizations, which sets that all persons and public, private, or mixed entities are obliged to cooperate in interception and access to data procedures provided for in articles 24 and 25 of the law.[46] The judge (*juez de garantías*) may impose fines when persons and entities fail to collaborate.

[44] Article 26, Law 121/2013, http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/95580/112588/F-86115861/PAN95580.pdf (Spanish) and Article 11, Law 51/2009, https://docs.panama.justia.com/federales/leyes/51-de-2009-sep-23-2009.pdf (Spanish).
[45] Articles 13 and 14, Law 51/2009.
[46] Article 27, Law 121/2013, http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/95580/112588/F-86115861/PAN95580.pdf (Spanish)

TRANSPARENCY & COMMUNICATIONS PRIVACY

13. Does the State report on the number of requests to access communications data?

No.

14. Is there any legal limitation that prohibits companies from publishing transparency reports?

To the best of our knowledge, no normative framework in Panama prohibits companies from publishing statistical data on the number of data requests made by the State. The country's law on transparency and access to information outlaws the release of restricted information for 10 years counted from its classification as such, which can be shorter, provided that the justifications for the restricted access cease to exist.[47] The kinds of information that can be restricted by the competent authority include those related to national security, handled by security institutions; judicial proceedings, only accessible by the parties until they are executed; and investigations carried out by police, intelligence, and other specified agencies.[48] This provision, however, cannot halt the release of statistical data, since they do not refer to a specific case, procedure, or document, but to aggregate, undetermined information.

15. Do telecommunication companies publish transparency reports?

- **Cable & Wireless Panamá (Más Móvil)** does not disclose transparency reports.

- **Movistar** released data about Panama's government data requests in Telefónica's 2018 transparency report. The local branch was sold to Millicom in 2019. Millicom's 2019 transparency report provides aggregated statistical data of government requests per region (Central America), not per country. The numbers related to Panama in the report do not include the newly acquired businesses.

- **Digicel** does not disclose transparency reports.

[47] Article 13, Law 6/2002 (*Ley 6 de 22 de enero de 2002 - Que dicta normas para la transparencia en la gestión pública, establece la acción de Habeas Data y dicta otras disposiciones*), https://www.antai.gob.pa/wp-content/uploads/2015/04/Ley-6-de-22-enero-2002.pdf (Spanish)
[48] Article 14, Law 6/2002.

- Claro does not disclose transparency reports.

16. Can companies notify users about States' data requests?

Companies can notify users beforehand about communications data requests when there is no secrecy obligation in effect. When this obligation exists, user notification can be carried out after the measure is completed or following deadlines set by law.

The Criminal Procedure Code states that no judicial decision produces legal effects before its notification to the parties.[49] However, resolutions that must be complied with immediately according to specific legal provisions are an exception and must be notified after their completion. Similarly, the judge (*juez de garantías*) has to examine the requests and issue the decisions in court hearings, even during the investigation phase, except for measures that by nature require confidentiality for fulfilling their purposes.[50] The Criminal Procedure Code states that obliged parties carrying out communications interception and recording must keep their content secret. It does not set, however, a secrecy obligation about the measure per se.[51] No secrecy obligation is set beforehand in Law 51/2009 either, which concerns the access to traffic and subscriber data.

Within investigations of criminal organizations, the prosecutor may determine the secrecy of proceedings for up to 30 days, by a reasoned decision, when keeping them public could hinder the investigation or cause the suspect to escape. It can be extended for equal periods, and the defense is entitled to request the judge to examine and terminate it. Despite the expiration of such deadlines, the judge may grant a prosecutor's request to carry out an investigative measure before hearing the suspect when this is necessary for its efficacy. The results must be informed to the defense, which, at least 30 days before the investigation is completed, must have access to the results of all secret proceedings.[52]

[49] Article 157, Criminal Procedure Code.
[50] Article 278, Criminal Procedure Code.
[51] Article 311, para 4, Criminal Procedure Code.
[52] Article 4, Law 121/2013, http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/95580/112588/F-86115861/PAN95580.pdf (Spanish)