FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Katie Porter
U.S. House of Representatives
1117 Longworth House Office Building
Washington, DC 20515

Dear Representative Porter:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Jamie Raskin
U.S. House of Representatives
2242 Rayburn House Office Building
Washington, DC 20515

Dear Representative Raskin:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Ayanna Pressley
U.S. House of Representatives
1108 Longworth House Office Building
Washington, DC 20515

Dear Representative Pressley:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Raúl M. Grijalva
U.S. House of Representatives
1511 Longworth House Office Building
Washington, DC 20515

Dear Representative Grijalva:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Adam B. Schiff
U.S. House of Representatives
2309 Rayburn House Office Building
Washington, DC 20515

Dear Representative Schiff:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Jackie Speier
U.S. House of Representatives
2465 Rayburn House Office Building
Washington, DC 20515

Dear Representative Speier:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Pramila Jayapal
U.S. House of Representatives
2346 Rayburn House Office Building
Washington, DC 20515

Dear Representative Jayapal:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Ed Case
U.S. House of Representatives
2210 Rayburn House Office Building
Washington, DC 20515

Dear Representative Case:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Ted Lieu
U.S. House of Representatives
403 Cannon House Office Building
Washington, DC 20515

Dear Representative Lieu:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Mondaire Jones
U.S. House of Representatives
1017 Longworth House Office Building
Washington, DC 20515

Dear Representative Jones:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Alexandria Ocasio-Cortez
U.S. House of Representatives
216 Cannon House Office Building
Washington, DC 20515

Dear Representative Ocasio-Cortez:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Grace Meng
U.S. House of Representatives
2209 Rayburn House Office Building
Washington, DC 20515

Dear Representative Meng:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Robin Kelly
U.S. House of Representatives
2416 Rayburn House Office Building
Washington, DC 20515

Dear Representative Kelly:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Eleanor Holmes Norton
U.S. House of Representatives
2136 Rayburn House Office Building
Washington, DC 20515

Dear Representative Norton:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Gwen Moore
U.S. House of Representatives
2252 Rayburn House Office Building
Washington, DC 20515

Dear Representative Moore:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Marc Veasey
U.S. House of Representatives
2348 Rayburn House Office Building
Washington, DC 20515

Dear Representative Veasey:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Jesús "Chuy" Garcia
U.S. House of Representatives
1519 Longworth House Office Building
Washington, DC 20515

Dear Representative Garcia:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Alan Lowenthal
U.S. House of Representatives
108 Cannon House Office Building
Washington, DC 20515

Dear Representative Lowenthal:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Gregory W. Meeks
U.S. House of Representatives
2310 Rayburn House Office Building
Washington, DC 20515

Dear Representative Meeks:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Norma J. Torres
U.S. House of Representatives
2227 Rayburn House Office Building
Washington, DC 20515

Dear Representative Torres:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Mark Takano
U.S. House of Representatives
420 Cannon House Office Building
Washington, DC 20515

Dear Representative Takano:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Dina Titus
U.S. House of Representatives
2464 Rayburn House Office Building
Washington, DC 20515

Dear Representative Titus:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Albio Sires
U.S. House of Representatives
2268 Rayburn House Office Building
Washington, DC 20515

Dear Representative Sires:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Suzanne Bonamici
U.S. House of Representatives
2231 Rayburn House Office Building
Washington, DC 20515

Dear Representative Bonamici:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Sanford D. Bishop
U.S. House of Representatives
2407 Rayburn House Office Building
Washington, DC 20515

Dear Representative Bishop:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Mark Pocan
U.S. House of Representatives
1727 Longworth House Office Building
Washington, DC 20515

Dear Representative Pocan:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Andy Levin
U.S. House of Representatives
312 Cannon House Office Building
Washington, DC 20515

Dear Representative Levin:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Rashida Tlaib
U.S. House of Representatives
1628 Longworth House Office Building
Washington, DC 20515

Dear Representative Tlaib:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Mary Gay Scanlan
U.S. House of Representatives
1227 Longworth House Office Building
Washington, DC 20515

Dear Representative Scanlan:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Donald M. Payne, Jr.
U.S. House of Representatives
106 Cannon House Office Building
Washington, DC 20515

Dear Representative Payne, Jr.:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Jim Cooper
U.S. House of Representatives
1536 Longworth House Office Building
Washington, DC 20515

Dear Representative Cooper:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Stephen F. Lynch
U.S. House of Representatives
2109 Rayburn House Office Building
Washington, DC 20515

Dear Representative Lynch:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Danny K. Davis
U.S. House of Representatives
2159 Rayburn House Office Building
Washington, DC 20515

Dear Representative Davis:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Hank Johnson
U.S. House of Representatives
2240 Rayburn House Office Building
Washington, DC 20515

Dear Representative Johnson:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Warren Davidson
U.S. House of Representatives
2113 Rayburn House Office Building
Washington, DC 20515

Dear Representative Davidson:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Earl Blumenauer
U.S. House of Representatives
1111 Longworth House Office Building
Washington, DC 20515

Dear Representative Blumenauer:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Yvette D. Clarke
U.S. House of Representatives
2058 Rayburn House Office Building
Washington, DC 20515

Dear Representative Clarke:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Mark DeSaulnier
U.S. House of Representatives
503 Cannon House Office Building
Washington, DC 20515

Dear Representative DeSaulnier:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Pete Aguilar
U.S. House of Representatives
109 Cannon House Office Building
Washington, DC 20515

Dear Representative Aguilar:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Carolyn B. Maloney
U.S. House of Representatives
2308 Rayburn House Office Building
Washington, DC 20515

Dear Representative Maloney:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Al Green
U.S. House of Representatives
2347 Rayburn House Office Building
Washington, DC 20515

Dear Representative Green:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable David Trone
U.S. House of Representatives
1110 Longworth House Office Building
Washington, DC 20515

Dear Representative Trone:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Sheila Jackson Lee
U.S. House of Representatives
2426 Rayburn House Office Building
Washington, DC 20515

Dear Representative Jackson Lee:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

March 7, 2022

The Honorable Rick Larsen
U.S. House of Representatives
2163 Rayburn House Office Building
Washington, DC 20515

Dear Representative Larsen:

Thank you for your letter regarding the collection and sale of consumers' location data. I share your concern that the unregulated commercialization of private geolocation data can compromise the safety and privacy of consumers. Location information is some of the most personal and sensitive data that carriers collect about their customers, and it must be safeguarded accordingly. That is why I want the Federal Communications Commission to use every tool at its disposal, including enforcement actions and rulemaking, to ensure that carriers protect the privacy of consumer location data and other sensitive customer information.

Under the Communications Act, the Commission has the ability to safeguard what is known as customer proprietary network information (CPNI). This is the "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer, solely by virtue of the carrier-customer relationship." It also includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." In more general terms, CPNI is the information, including location data, that telecommunications carriers have about their customers as a result of their unique position as network operators.

The agency's Enforcement Bureau investigates lapses in privacy protection associated with CPNI, which often arise in the context of data breaches. The agency has the ability to strengthen its rules in response to such lapses, provided any changes are consistent with the Communications Act. On CPNI matters, the Commission regularly coordinates with other law enforcement entities, including the Federal Trade Commission, through formal quarterly coordination and more informally, when warranted by specific cases.

In addition, the Enforcement Bureau requires carriers to certify compliance with the Commission's CPNI rules on an annual basis. This yearly certification includes a statement from the telecommunications carrier explaining its CPNI practices as well as a summary of complaints concerning any unauthorized release of CPNI.

In 2020, the Commission issued a series of Notices of Apparent Liability for Forfeiture against the major wireless carriers for disclosing customer location information. The location

information disclosed by the carriers had made its way into the hands of bounty hunters and other unscrupulous entities. In the wrong hands, this sensitive data could be used to facilitate criminal activity, stalking, and the release of sensitive information with security consequences. The Commission's actions against the wireless carriers made clear that every carrier has a duty to keep location data private as part of its statutory duty to protect CPNI. Moreover, the Commission determined that failing to take reasonable measures to protect consumer location information violates the Communications Act and the agency's CPNI rules. As a result, carriers that fail to reasonably protect customer location data and other CPNI will be investigated and subject to enforcement action by the Commission.

As a Commissioner, I believed the agency could have done more to hold carriers accountable for failures to adequately protect CPNI, including location information. As a result, as Chairwoman, I have introduced measures to strengthen our CPNI rules in response to developing threats to consumer privacy.

To this end, in September 2021, the Commission adopted a rulemaking seeking comment on specific proposals to update our rules to better protect consumers from the fraudulent transfer of phone numbers, through SIM swapping or "port-out" fraud. These scams typically involve a bad actor taking control of a consumer's telephone number in order to reset passwords to facilitate theft from financial accounts.

In addition, in January 2022, I shared with my colleagues a proposal for a rulemaking that, if adopted, would update and improve the Commission's rules for notifying customers and federal law enforcement of data beaches affecting CPNI. Specifically, the rulemaking would require that customers are notified of data breaches without unreasonable delay, which is particularly important in light of the increased frequency of data breaches. Our current rules, which date to 2007, require that carriers wait at least seven full business days before notifying customers. The rulemaking that I have shared with my colleagues would also propose to extend the breach notification requirement to inadvertent breaches of information, recognizing that breaches can harm customers regardless of whether they are intentional or not.

Thank you for your attention to this matter. The Commission remains committed to protecting the privacy of consumer data, including location data. We will continue to enforce the consumer protection policies in the Communications Act and implement new rules when needed. We also would be happy assist you and your office, should you wish to consider changes to the laws governing these matters. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel