epic.org

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

June 11, 2013

Acting Chairwoman Mignon Clyburn
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Dear Chairwoman Clyburn:

We are writing to you regarding privacy protections for American telephone customers and recent news reports that Verizon, one of the largest domestic phone companies subject to the Commission's regulations, has unlawfully disclosed call detail information to the National Security Agency ("NSA"). *The Guardian* reported that in response to a Foreign Intelligence Surveillance Court ("FISC") order, Verizon released identifying call information in real-time to the NSA, including telephone numbers and time and call duration.[1] *The Guardian* also published a copy of the order.[2] By surrendering protected information of its consumers in response to a facially invalid order, Verizon has violated the legal protections surrounding consumer proprietary network information ("CPNI"). Accordingly, we ask that the Commission begin an investigation.

The Electronic Privacy Information Center ("EPIC") is a non-partisan research organization, established in 1994 to focus attention on emerging privacy and civil liberties issues.[3] EPIC has worked closely with the FCC in the past to establish privacy safeguards for telephone customers, having brought the issue of call records sales to the attention of the Commission in 2005, and having supported the subsequent rulemaking on the issue.[4] More recently, EPIC submitted extensive comments to the Commission, making recommendations concerning privacy and security of information stored on mobile communications devices.[5]

We are writing now to urge you to open an investigation into Verizon's decision to turn over call records to the NSA without legal authority. This action also violated Section 222 of the Telecommunications Act of 1996, which mandates that telecommunications carriers, such as Verizon, protect CPNI.[6] As discussed in detail below, Verizon's CPNI disclosure to the NSA violates Section 222's restriction on disclosures. Accordingly, the Commission should turn its attention to the significant

---

[1] *Verizon Forced to Hand Over Telephone Data – Full Court Ruling*, THE GUARDIAN (June 5, 2013, 7:04 PM) http://www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephone-data-court-order.
[2] *In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Serv., Inc. on Behalf of MCI Commc'n Serv., Inc. D/B/A Verizon Bus. Serv.*, Dkt. No. BR 13-80 at 1-2 (FISA Ct. Apr. 25, 2013), *available at* http://epic.org/privacy/nsa/Section-215-Order-to-Verizon.pdf.
[3] EPIC, *About EPIC*, http://epic.org/epic/about.html (last visited June 6, 2013).
[4] Petition from EPIC to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005); Comments from EPIC *et al*. on the Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (Apr. 14, 2006).
[5] Comments from EPIC *et al*. on Privacy and Security of Information Stored on Mobile Communications Devices, CC Docket No. 96-115; DA 12-818 (July 13, 2012), *available at* http://epic.org/privacy/location_privacy/EPIC-FCC-Mobile-Privacy-Comments.pdf.
[6] Telecommunications Act of 1996, 47 U.S.C. § 222 *et seq*.

communications privacy issues arising from Verizon's massive disclosure of legally protected, sensitive consumer information.

We have attached a copy of the order issued by the Foreign Intelligence Surveillance Court to Verizon to this letter for your review.

Section 222 of the Telecommunications Act Requires That Telecommunications Carriers Protect the Privacy Rights of Customers by Limiting Access to CPNI

Section 222 of the Communications Act requires the telecommunications carriers to "protect the confidentiality of proprietary information of, and relating to . . . customers."[7] The Act defines three types of personal information: customer proprietary network information ("CPNI") aggregate information, and subscriber list information. CPNI includes the time, date, duration, destination number, and location of telephone calls, and any other information that appears on the subscriber's telephone bill.[8] As the Commission recognizes, "Congress accorded CPNI, the category of customer information at issue in this Order, the greatest level of protection under this framework."[9]

The law places strict limits on telecommunications carriers' ability to disclose CPNI. Disclosure is only permitted as required by law, with the customer's consent, or pursuant to four narrowly-drawn exceptions related to the facilitation of telecommunications or emergency services.[10]

Verizon Violated the Telecommunications Act and the Privacy of its Customers

The government obtained an order under Section 215 of the Patriot Act that covered "Telephony metadata," which "includes, *inter alia*, the "originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number . . . time and duration of call."[11] Because telephony metadata includes telephone numbers, call times, locations, and durations, by surrendering this information to the government, Verizon disclosed the CPNI of millions of consumers.

Verizon's disclosure of CPNI to the NSA was not authorized under the Telecommunications Act because it did not fall under any of the Act's permissible disclosures. Verizon customers did not authorize these disclosures. And as we detailed in our letter to Congress, the FISC order was not lawful.[12] The Foreign Intelligence Surveillance Act ("FISA") is intended to authorize the Intelligence Community to engage in *foreign* intelligence gathering, not domestic.[13] The FISC is supposed to ensure that FISA

---

[7] 47 U.S.C. §222 (a).
[8] 47 U.S.C. § 222 (h)(1)(A)-(B).
[9] Telecomm. Carriers' Use of Customer Proprietary Network Info. And Other Customer Info., Rpt. And Order and Further Notice of Proposed RM, 22 F.C.C.R. 6927 (2007), http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf
[10] 47 U.S.C. §§ 222 (c)(1); (d)(1)-(4)
[11] *In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Serv., Inc. on Behalf of MCI Commc'n Serv., Inc. D/B/A Verizon Bus. Serv.*, Dkt. No. BR 13-80 at 2 (FISA Ct. Apr. 25, 2013) (hereinafter "Verizon Order"), *available at* http://epic.org/privacy/nsa/Section-215-Order-to-Verizon.pdf.
[12] Letter from EPIC to Congress (June 7, 2013), *available at* http://epic.org/FISC-NSA-domestic-surveillance.pdf (concerning NSA Domestic Surveillance Oversight).
[13] "This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused." S. Rep. No. 95-604(I) at 7 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908.

investigations do not focus on U.S. persons. This order does not satisfy those purposes and directly violates the FISA's legal requirements.

The role of carriers like Verizon is particularly important because the structure of the Foreign Intelligence Surveillance Act does not allow for meaningful public oversight or accountability. The Attorney General's annual FISA report provides virtually no meaningful information about the use of FISA authority other than the applications made by the government to the Foreign Intelligence Surveillance Court.[14] There is no information about cost, purposes, effectiveness, or even the number of non-incriminating communications of US persons that are collected by the government. And the government refuses even to disclose its legal interpretation of Section 215, which led Senators Wyden and Udall to reveal that "there is now a significant gap between what most Americans *think* the law allows and what the government *secretly claims* the law allows."[15]

More importantly, Section 215 deprives the subjects of surveillance of notice and an opportunity to challenge the orders. The law prevents those served with Section 215 orders from disclosing this fact to anyone else.[16] And unlike physical searches, electronic surveillance routinely occurs without any noticeable disturbance to the target or to innocent bystanders whose personal communications are intercepted.[17] Thus, millions of consumers had no way of knowing that their personal information had been illegally provided to the NSA by Verizon.

Without notice, these consumers are completely dependent on Verizon for the protection of their personal phone records. Verizon has refused to provide information about its role in abetting NSA surveillance, instead issuing evasive, misleading denials. In 2006, the company stated that it would not provide "unfettered access to our customer records or provide information to the government under circumstances that would allow a fishing expedition."[18] But it appears that is exactly what has occurred. In response to the current NSA spying revelations, Verizon said that "the law authorizes the federal courts to order a company to provide information in certain circumstances, and if Verizon were to receive such an order, we would be required to comply."[19] However, Verizon's compliance need not be automatic: Section 215 allows a company to challenge the government's production request,[20] and when faced with a plainly illegal order, this is what the CPNI protections obligate the company to do.

---

[14] It is clear from the Attorney General's annual reports that FISC applications are routinely approved with very rare exceptions. See Amnesty Int'l USA v. Clapper, 638 F.3d 118, 140 (2d Cir. 2011) ("Empirical evidence supports this expectation: in 2008, the government sought 2,082 surveillance orders, and the FISC approved 2,081 of them."). Of the Government's 1,676 requests to the FISC for surveillance authority in 2011, none were denied in whole or in part. See Letter from Assistant Attorney General Ronald Weich to Joseph Biden, President, United States Senate, Apr. 30, 2012 ("2011 FISA Annual Report to Congress"), http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf.

[15] Letter from Senator Mark Udall and Senator Ron Wyden, United States Senate, to the Honorable Eric Holder, Attorney General, United States Dep't of Justice (Mar. 15, 2012), *available at* https://www.documentcloud.org/documents/325953-85512347-senators-ron-wyden-mark-udall-letter-to.html.

[16] USA PATRIOT Act of 2001 § 215, 50 U.S.C. §§ 1861(d)(1) (2006).

[17] Whitfield Diffie and Susan Landau, Privacy on the Line 175 (2007) (""It is inherent in telecommunication—and inseparable from its virtues—that the sender and receiver of a message have no way of telling who else may have recorded a copy.")

[18] Press Release, Verizon, Verizon Issues Statement on NSA and Privacy Protection (May 11, 2006), http://newscenter2.verizon.com/press-releases/verizon/2006/page-29670741.html.

[19] Randy Milch, *From the desk of Randy Milch*, VERIZON POLICY BLOG (June 6, 2011), http://publicpolicy.verizon.com/blog/entry/from-the-desk-of-randy-milch.

[20] 50 U.S.C. §§ 1861f(1)(2)(A)(i).

The Commission has the Obligation to Protect the Privacy of Consumers' Phone Records

The Commission should investigate Verizon's violations of the Telecommunications Act, and its consumers' privacy, by surrendering protected information in response to a plainly unlawful order. In passing the Communications Act, Congress gave the Commission broad investigative, regulatory, and enforcement powers.[21] In particular, Congress charged the FCC with implementing the CPNI protections contained in the Communications Act. Over twenty years ago, the Commission ruled that CPNI "belongs to the customers," not carriers, and restricted carriers' use of CPNI.[22] Since then, the Commission has exercised its authority numerous times to protect the privacy of consumers' phone records.[23] Former Chairman Genachowski has stated, "The right to privacy is a core American value, and the Federal Communications Commission, at the direction of Congress, has worked for years to implement laws that protect the privacy of consumers when they use communications networks."[24]

And you recently affirmed the Commission's dedication to consumer privacy rights when you stated, "[m]illions of wireless consumers must have confidence that personal information about calls will remain secure even if that information is stored on a mobile device."[25]

Conclusion

The Commission plays a critical role in safeguarding the privacy of American consumers. We look forward to hearing from you as soon as possible regarding the action the FCC intends to take.

Sincerely,

Marc Rotenberg
EPIC Executive Director

Khaliah Barnes
EPIC Administrative Law Counsel

David Jacobs
EPIC Consumer Protection Counsel

Enclosure: Verizon Order

[21] *See* 47 U.S.C. §151.
[22] AT&T, 102 FCC 2d 655 (1985)
[23] *See, e.g.*, Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 (1998); Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860 (2002); Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007).
[24] Julius Genachowski, Chairman, Fed. Commc'n Comm., Statement at House Hearing on "Internet Privacy: The Views of the FTC, the FCC and NTIA (July 14, 2011), *available at* http://www.fcc.gov/document/genachowski-statement-house-hearing-internet-privacy.
[25] Brendan Sasso, *FCC to Vote on Cellphone Privacy Rules*, THE HILL (June 5, 2013, 2:31 PM), http://thehill.com/blogs/hillicon-valley/technology/303643-fcc-to-vote-on-cellphone-privacy-rules?utm_source=twitterfeed&utm_medium=twitter