District Court, [Redacted] , State of Colorado	
In Re Marriage of: Petitioner: [Redacted] v. Respondent: [Redacted]	
Attorney for Electronic Privacy Information Center: Guilherme Roschke, NY Bar no 4486403 Electronic Privacy Information Center 1718 Connecticut Ave NW #200 Washington DC 20009 Tel: 202-483-1140 x124 Fax: 202-483-1248 Email:roschke@epic.org	Case No: [Redacted]
Motion for Leave to File Brief of Amicus Curiae Electronic Privacy Information Center in Support of Petitioner.	

The Electronic Privacy Information Center hereby moves for leave to file the included brief of amicus curiae pursuant to Colorado Appellate Rule 29.

Statement of Interest and Desirability

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. that was established in 1994 to focus public attention on emerging civil liberties issues. EPIC has participated as *amicus curiae* in numerous privacy cases, including *Hiibel v. Sixth Judicial District Court of Nevada,* No. 03-5554 (2004), *Doe v. Chao*, 124 S. Ct. 1204 (2004), *Smith v. Doe*, 538 U.S. 84 (2003), *Dep't of Justice v. City of Chicago*, 537 U.S. 1229 (2003), *Watchtower Bible and Tract Soc'y of*

N.Y. Inc. v. Vill. of Stratton, 536 U.S. 150 (2002), *Reno v. Condon*, 528 U.S. 141 (2000).

EPIC files this brief to inform the court of the growing public policy support for the privacy of telephone record information, as reflected in a recent order of the Federal Communications Commission and recent Acts of Congress, as well as the range of privacy interests that are implicated by the Magistrate's Order for the production of cell phone records.

EPIC respectfully requests to present this information to the court via e-filing and service accomplished by counsel for the petitioner.

Respectfully Submitted,

Electronic Privacy
Information Center

BY:_____

Guilherme Roschke
NY Bar no:4486403
Attorney for Electronic
Privacy Information Center

1718 Connecticut Ave NW #200
Washington DC 20009
Tel: 202-483-1140 x124
Fax: 202-483-1248
Email:roschke@epic.org

(to be e-filed and served on respondent by attorney for petitioner)

District Court, [Redacted] , State of Colorado	
In Re Marriage of: Petitioner: [Redacted] v. Respondent: [Redacted]	
Attorney for Electronic Privacy Information Center: Guilherme Roschke, NY Bar no 4486403 Electronic Privacy Information Center 1718 Connecticut Ave NW #200 Washington DC 20009 Tel: 202-483-1140 x124 Fax: 202-483-1248 Email:roschke@epic.org	Case No: [Redacted]
Brief of Amicus Curiae Electronic Privacy Information Center in Support of Petitioner	

Summary of the Argument

There is a strong and growing public policy consensus that recognizes the heightened privacy interest of telephone records and seeks to limit the circumstances under which such records may be disclosed. Moreover, recent actions by the Federal Communications Commission and the U.S. Congress protect not just a general privacy interest in these records, but also recognize the physical and emotional safety needs of the subjects of these records. These developments are relevant to the Court's considerations in this matter.

Courts are to employ a balancing test when resolving discovery issues. *Leidholt v. District Court in and for City and County of Denver*, 619 P.2d 768, 770 (Colo. 1980). The Court "may make any order which justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense . . . ." C.R.C.P 26(c). Specifically concerning privacy and confidentiality, courts are to engage in a three part balancing test: "(1) whether the individual has a legitimate expectation of non-disclosure; (2) whether disclosure is nonetheless required to serve a compelling sate interest; and (3) where a compelling state interest necessitates disclosure of otherwise protected information, how disclosure may occur in a manner which is least intrusive with respect to confidentiality." *Corbetta v. Albertson's, Inc.*, 975 P.2d 718, 720-221 (Colo. 1999).

Amicus EPIC therefore respectfully requests that this Court reverse the Magistrate's Order and grant Petitioner's motion for a protective order where Respondent has sought "Any and all documentation of [Petitioner's] cell phone records, including but not limited to names, dates, and numbers, for the past five years."

EPIC's Interest in Protecting Telephone Records.

A substantial amount of EPIC's work has been directed at defending the privacy of telephone records. *See* EPIC's Page on the Illegal Sale of Phone Records, http://www.epic.org/privacy/iei/. EPIC has filed a successful petition to the Federal Communications Commission (FCC) concerning the illegal sale of telephone

records. In re *Implementation of the Telecommunications Act of 1996*, Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Costumer Proprietary Network Information, CC Docket No. 96-115 (Aug. 30, 2005), http://epic.org/privacy/iei/cpnipet.html. The FCC has responded to our petition with a new order and proposed rulemaking, discussed below, that established new limitations on the disclosure of information of the type at issue in this matter,.

In *Conboy v. AT&T*, 241 F. 3d 242 (2d Cir, 2002), a case concerning the disclosure of unlisted number, home address and telephone billing information, we argued that courts have recognized the harm that flows from the unauthorized disclosure of personal information and have expanded privacy protections in response to new threats to this fundamental right. Brief for Electronic Privacy Information Center as Amici Curiea Supporting Appellants, http://www.epic.org/privacy/consumer/conboy_brief.html.

In our efforts to defend the privacy of telephone records from unauthorized access, EPIC has recognized the importance of the neutral review offered by judicial process. *See eg.* Letter to Senator Bowen from Electronic Privacy Information Center on SB 1666, (Apr. 24, 2006) http://www.epic.org/privacy/iei/sb166632406.html. We therefore respectfully urge this Court, as part of the *Corbetta* review, to consider recent developments that underscore the privacy interest that an individual has in restricting the disclosure of telephone record information.

A Recent FCC Order Recognizes the Privacy Interest In Telephone Records and Promotes Individual Control.

Section 222 of The Telecommunications Act of 1996 requires telecommunications carriers to protect the confidentiality of proprietary information of and relating to its costumers. 47 U.S.C. § 222(a). Elevated protection is provided for Costumer Proprietary Network Information (CPNI). *Id.* at § 222(c)(1). CPNI includes among other things, the calling records of incoming and outgoing calls. *Id.* at § 222(h)(3). Specifically, carriers that receive CPNI by virtue of providing a telecommunication service may only use, disclose, or permit access to this CPNI for the provision of the telecommunication service or other services necessary or used in the provision of the telecommunications service. *Id.* at § 222(c)(1).

In taking regulatory action to carry out the mandates of § 222, the Federal Communications Commission (FCC) recently strengthened its privacy rules by proposing new safeguards. In re *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (April 2, 2007), http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf. EPIC had previously filed a complaint with the FCC, and it was EPIC's petition that led to this order. *Id.* at 3.

The FCC's order included a significant change in the protection of telephone records, recognizing the need for

individuals to control their own records. The order mandated that carriers change from an "opt-out" to an "opt-in" policy for the disclosure of records to joint venture partners and contractors. *Id.* at 22. Among the specific findings is that opt-in "directly and materially advances privacy and safety interest by giving customers direct control over the distribution of their private information." *Id.* at 25. Though the FCC's order is heavily aimed at "pretexting" of consumer of consumer information, they note that the purpose is to stop all forms of unauthorized disclosure: "Unauthorized disclosure of CPNI by any method invades the privacy of unsuspecting consumers and increases the risk of identity theft, harassment, stalking, and other threats to personal safety." *Id.* at 26.

The statements of the FCC commissioners demonstrate a strong public interest in protecting the privacy of telephone records. In a statement accompanying the Order, FCC Chairman Kevin J. Martin wrote "[t]he unauthorized disclosures of consumers' private calling records is a significant privacy invasion." *Id.* at 95. Commissioner Michael J. Copps stated "[f]ew rights are as fundamental as the right to privacy in our daily lives, but this cherished right seems under almost constant attack. As recent abuses by unscrupulous data brokers and others illustrate, the Commission's existing customer proprietary network information (CPNI) rules have not adequately protected individual privacy." *Id.* at 96. Commissioner Jonathan Adelstein declared "[t]hrough this proceeding, we address an issue of immediate personal importance to American consumers, the protection of sensitive information that telephone companies collect about their costumers."

Congress Has Recently Issued Findings and Enacted Legislation on the Protection of Telephone Records

Congress recently strengthened the privacy of telephone records information with the enactment of the Telephone Records and Privacy Protection Act of 2006. Pub. L. No. 109-476, 120 Stat. 3568 (2007) (codified at 18 U.S.C. § 1039). The Act criminalized the pretexting of telephone records. *Id.* at 3569, § 3(a). The Act also criminalized was the sale, transfer and receipt of confidential records accessed via such pretexting. *Id.* at §§ 3(b), 3(c). Congress found that personal data can be valuable to criminals. *Id.* at 3568, § 2(1). Significantly, Congress also found that these disclosures do not just threaten privacy, they are used to further domestic violence and stalking, and otherwise compromise the safety of individuals. *Id.* at § 2(5).

The Violence Against Women Act Recognizes the Value of Being Free From Tracking.

The Violence Against Women Act Reauthorization expanded the definition of criminal stalking to recognize that access to personal information such as telephone records creates specific risks of harm. The Act added to the definition of stalking "plac[ing] under surveillance with intent to kill, injure, harass, or intimidate another person." Pub. L. No 109-162, 119 Stat. 2960, 2987, § 114(a) (2005) (providing new language for 18 U.S.C. § 2261A).

This significant change recognizes the privacy interest one has in most of their daily activities, even if carried out in public. The change recognizes that surveillance can be used for, and can cause, harassment and intimidation. It recognizes that placing someone under scrutiny and observation can be used to harass and intimidate. Besides the general anxiety and discomfort that surveillance can cause, in instances of stalking it creates a direct fear for one's physical safety, and for the safety of relationships that the surveillance exposes.

Colorado Law on Stalking also Protects Individuals from Surveillance:

Colorado law on stalking punishes one that "Repeatedly . . . places under surveillance . . . in a manner that would cause a reasonable person to suffer serious emotional distress and does cause that person . . .to suffer serious emotional distress" with the requisite intent. Colo. Rev. Stat. §18-9-111(4)(b)(III) (2007). A court addressed this definition in the example of defendant that used a Global Positioning System (GPS) device to track the movements of his victim's car. *People v. Sullivan*, 53 P.3d 1181 (Colo. Ct. App. 2002). The court noted that the legislature had "the goal of encouraging and authorizing effective intervention before stalking can escalate into behavior that has even more serious consequences." *Id.* at 1183-84. Surveillance of communication raises the same concern of early intervention as communication surveillance reveals a person's contacts, friends and associates.

Privacy Interests Include Security and Use Limitation, Not Just Confidentiality.

Privacy policy is also concerned with maintaining data securely and limiting secondary uses. These two principles are part of the five principles of Fair Information Practices, first developed in the 1970's:

- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

U.S. Dep't of Health, Educ. & Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Comm. On Automated Personal Data Systems*, 41-42 (1973)

In other words, data requested for a specific purpose should be used only for that purpose, with some meaningful way that the subject of the data can guarantee that this purpose limitation. Furthermore, those holding or collecting data on individuals are responsible for keeping this data secure and correct.

These principles are directly implemented in public policy. The FCC Order described above contains detailed

regulations for the steps telecommunications carriers must take to keep data secure. The Federal Trade Commission (FTC) has also used its unfairness and deception authority to maintain data security. *See* Federal Trade Commission, *Privacy Initiatives: Unfairness and Deception, Enforcement*, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (listing FTC enforcement actions against businesses that fail to maintain costumer data secure from breach and disclosure).

Policy also reflects a will to prevent secondary uses. As mentioned above, the Telecommunications act requires that carriers that receive CPNI by virtue of providing a telecommunication service may only use, disclose, or permit access to this CPNI for the provision of the telecommunication service or other services necessary or used in the provision of the telecommunications service. 47 U.S.C. § 222(c)(1). This reflects the principle that the data collection is legitimate for a given purpose, and disclosure should be seen in the context of the purpose of the disclosure.

Conclusion:

There is a strong and growing public policy towards the protection of telephone records. This policy recognizes the sensitivity of this information to individuals. Secondly, preventing someone from tracking one's daily life and communication is a recognized interest whose violation can cause emotional harm. Lastly, ones privacy interest in data is not limited to simply maintaining it confidential from a given party, but also includes other concepts such

as security and use limitation. We urge the court to include these interests as it applies its balancing test.

Respectfully Submitted,

Electronic Privacy
Information Center

BY:_____

Guilherme Roschke
NY Bar no:4486403
Attorney for Electronic
Privacy Information Center
1718 Connecticut Ave NW #200
Washington DC 20009
Tel: 202-483-1140 x124
Fax: 202-483-1248
Email:roschke@epic.org

(to be e-filed and served on respondent by attorney for petitioner)