VIRGINIA LAW REVIEW ONLINE

VOLUME 102 SEPTEMBER 2016 101–112

ESSAY

DATA PRIVACY AND INMATE RECIDIVISM

Chad Squitieri[*]

INTRODUCTION

WHEN one thinks of prison, the concept of privacy does not generally come to mind. Indeed, the Panopticon imagined by English philosopher Jeremy Bentham—a prison designed in such a way that no inmate could be certain whether he was currently being watched—has become reality.[1] While Bentham envisioned a centralized "inspector" with the ability to peer into the prison cells that surrounded him,[2] modern Internet-connected technologies have allowed today's inspectors to surveil inmates regardless of their physical proximity.

But while the introduction of Internet-connected technologies into correctional facilities has enhanced the surveillance capabilities of the *watchers*, it has also provided value to the *watched*. The introduction of video-messaging services, for example, has allowed inmates to communicate with loved ones who are unable to travel to visit in person.[3]

[*] J.D., 2016, University of Virginia School of Law. I would like to thank Professors Chris Hoofnagle and Frank Pasquale for their feedback on earlier drafts of this Essay. Any remaining errors are mine. The views expressed in this Essay are my own, and do not necessarily reflect the views of my employer or its clients.

[1] Thomas McMullan, What Does the Panopticon Mean in the Age of Digital Surveillance?, Guardian (July 23, 2015), http://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham [https://perma.cc/435Q-6BVF].

[2] Jeremy Bentham, Panopticon: Or, the Inspection-House 4–5 (Dublin, Thomas Byrne 1791).

[3] See, e.g., Emily Green, Captive Consumers: Corporations Reap Big Profits on Inmate Finances, Video Visitation in Multnomah County, Street Roots News (Jan. 6, 2015),

Indeed, the private companies that obtain government contracts to introduce these Internet-connected technologies into correctional facilities often argue that their services can reduce recidivism rates by providing inmates with the opportunity to engage in such communication services.[4] A close examination of the privacy policies offered by these correctional contractors, however, reveals how efforts to reduce recidivism rates are undermined.

As this Essay will explain, correctional contractors collect sensitive data about inmates and the loved ones with whom they communicate. If this data is stolen or sold it can result in substantial harm. Allowing mistaken or misleading data to end up in the hands of an employer or would-be creditor, for example, can undermine efforts to successfully integrate former inmates back into society. Similarly, even accurate data that links individuals with their prior criminal acts can result in former inmates facing burdens in credit and labor markets long after they have paid their debt to society. As research continues to examine the cyclical relationship between incarceration and poverty, placing additional burdens on former inmates in credit and labor markets means placing additional burdens on society's interest in reducing recidivism rates and lifting families out of poverty.[5] The privacy policies currently offered by correctional contractors do not protect against these problems. This Essay therefore calls on the Federal Communications Commission ("FCC") to correct such harms.

Having recently set out to establish the maximum rates that correctional contractors can charge inmates for telephone services,[6] the FCC is the appropriate entity to regulate the Internet services that these correctional contractors also provide. Indeed, the FCC has already sought comment on "[t]he use, costs and rates of video visitation and other advanced inmate communications . . . and whether these services could be

http://news.streetroots.org/2015/01/06/captive-consumers-reap-big-profits-inmate-finances-video-visitations [https://perma.cc/G687-N9ET].

[4] Securus Technologies, Inc. to Acquire JPay Inc., PR Newswire (Apr. 14, 2015, 11:30 AM), http://www.prnewswire.com/news-releases/securus-technologies-inc-to-acquire-jpay-inc-300065531.html [https://perma.cc/J98A-STHM].

[5] See Sasha Abramsky, Toxic Persons, Slate (Oct. 8, 2010, 7:34 AM), http://www.slate.com/articles/news_and_politics/jurisprudence/2010/10/toxic_persons.html [https://perma.cc/SD7J-CVP6].

[6] Jon Brodkin, FCC Will Let Jails Charge Inmates More for Phone Calls, Ars Technica (July 18, 2016, 12:55 PM), http://arstechnica.com/tech-policy/2016/07/fcc-will-let-jails-charge-inmates-more-for-phone-calls/ [https://perma.cc/2ZUX-PQZV].

used to circumvent traditional [inmate calling services] rates."[7] While establishing rate caps for Internet services is an important step, this Essay calls on the FCC to regulate Internet services within correctional facilities on two additional fronts. First, the FCC should prohibit correctional contractors from selling the data they collect to private third parties. Second, the FCC should establish clear liability guidelines holding correctional contractors liable for data breaches.

Part I will examine the current landscape in which these correctional contractors have introduced their services into correctional facilities. Doing so reveals the financial incentives that state and local governments have to grant contracts with inadequate privacy policies, elucidating the need for federal intervention. Part II will then address how current privacy policies offer inmates and their loved ones inadequate protection, and propose how the FCC can act to require increased privacy protections.

I. LANDSCAPE

Many correctional facilities now permit inmates to access the Internet.[8] One interest that state and local governments have in doing so is that permitting such access can reduce recidivism rates. Permitting access to online educational tools, for example, can provide inmates with marketable skills they can use to secure stable employment after their release.[9] Similarly, allowing inmates to communicate with loved ones can help foster supportive relationships.[10] Indeed, the FCC has acknowledged that "contact between inmates and their loved ones has been shown to reduce the rate of recidivism."[11]

[7] Press Release, FCC, FCC Takes Next Big Steps in Reducing Inmate Calling Rates (Oct. 22, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-335984A1.pdf [https://perma.cc/C2R4-8R6B].

[8] Ben Branstetter, The Case for Internet Access in Prison, Wash. Post (Feb. 9, 2015), https://www.washingtonpost.com/news/the-intersect/wp/2015/02/09/the-case-for-internet-access-in-prisons/ [https://perma.cc/M6KV-YEKE].

[9] Anne Field, Startup's Education Platform for Curbing Recidivism Launches Pilot in Philly Prison, Forbes, Oct. 31, 2014, http://www.forbes.com/sites/annefield/2014/10/31/startups-education-platform-for-curbing-recidivism-launches-pilot-in-philly-prison/ [https://perma.cc/76NH-9X5M].

[10] Margaret diZerega & Sandra Villalobos Agudelo, Vera Inst. of Justice, Piloting a Tool for Reentry: A Promising Approach to Engaging Family Members 4 (2011), http://www.vera.org/sites/default/files/resources/downloads/Piloting-a-Tool-for-Reentry-Updated.pdf [https://perma.cc/5NX6-U6SY].

[11] Press Release, FCC, supra note 7.

State and local governments, however, also have a troubling incentive to introduce these services: Correctional facilities often supplement their budgets with kickback payments based on a correctional contractor's profits.[12] Indeed, these payments appear to be so substantial that some correctional contractors have sued to stop the implementation of the FCC's rate caps on telephone services, arguing that the caps are too low to allow the contractors "to recoup the . . . payments that they are contractually obligated to make [to correctional facilities]."[13] Because correctional contractors can increase their profits by selling their customers' data, correctional facilities have the financial incentive to approve privacy policies that allow for such sales, thus undermining efforts to reduce recidivism rates. Part I will address this financial incentive in greater detail and outline the authority under which the FCC can regulate this relationship.

A. Current Legal Framework

Since Justice Harlan's announcement in *Katz v. United States* that the Fourth Amendment protects an individual's "reasonable expectation of privacy,"[14] the Fourth Amendment has offered a constitutional grounding for privacy protections. As time would reveal, however, this constitutional grounding was rather unsteady, and the Court has since resorted to crafting an intricate web of context-specific rules to define "reasonable expectation of privacy."[15] One such rule addresses how the Fourth Amendment applies in correctional facilities. In *Hudson v. Palmer* the Court held that inmates have no "reasonable expectation of privacy in [their] prison cell entitling [them] to the protection of the Fourth Amendment against unreasonable searches and seizures."[16]

As the Court made clear in *Palmer*, correctional facilities are not typically thought of as privacy havens, nor should they be. The Court in

[12] Stephanie Clifford & Jessica Silver-Greenberg, In Prisons, Sky-High Phone Rates and Money Transfer Fees, N.Y. Times (June 26, 2014), http://www.nytimes.com/2014/06/27/business/in-prisons-sky-high-phone-rates-and-money-transfer-fees.html?_r=0 [https://perma.cc/6MCM-PPUA].

[13] Motion of Global Tel*Link for Partial Stay Pending Judicial Review at 9, Global Tel*Link v. FCC (D.C. Cir. 2016) (No. 15-1461), http://cdn.arstechnica.net/wp-content/uploads/2016/03/prison-phone-stay-petition.pdf [https://perma.cc/KX5L-898P].

[14] 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

[15] Orin S. Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 Harv. L. Rev. 476, 479–80 (2011).

[16] 468 U.S. 517, 519 (1984).

Palmer, however, did not declare that inmates have *no* legitimate interest in privacy. Instead, the Court simply held that any privacy interest that an inmate might have would need to be derived from a source other than the Fourth Amendment. This Essay therefore suggests a regulatory framework designed to offer privacy protections where the Fourth Amendment fails to do so.

B. The Need for Federal Regulation and the FCC's Authority

As state and local budgets came under greater scrutiny during the Great Recession, correctional facilities increasingly sought new sources of funding.[17] Correctional contractors provided one such source, offering to pay correctional facilities a portion of their profits through kickback payments.[18] These kickback payments led state and local governments to develop a financial incentive that directly conflicts with the interests of inmates and their loved ones, as well as society's long-term interest in reducing recidivism rates. This conflict has resulted in a need for federal action, a need that the FCC began to fulfill in October 2015 when it set out to cap the rates at which correctional contractors can charge for telephone services.[19] The FCC should similarly regulate Internet services—services often provided by the same companies that provide telephone services in correctional facilities.[20]

Though fundamental principles of federalism require a pragmatic approach to considering federal regulation of state correctional systems, Internet services are hardly an intrastate matter. Not only do the communications themselves travel across state boundaries, the effects on inmates are not contained within the state in which inmates are incarcerated. As the federal agency tasked with regulating Internet service providers, the FCC has the authority to regulate Internet services provided by correctional contractors. The FCC's authority to do so derives primarily from Section 706 of the Telecommunications Act, which requires

[17] Patrice A. Fulcher, The Double-Edged Sword of Prison Video Visitation: Claiming to Keep Families Together While Furthering the Aims of the Prison Industrial Complex, 9 Fla. A&M U. L. Rev. 83, 85–87 (2013).

[18] Clifford & Silver-Greenberg, supra note 12.

[19] Press Release, FCC, supra note 7.

[20] Matt Stroud & Joshua Brustein, Expensive 'Prison Skype' Is Squeezing Out In-Person Visitation, Bloomberg News (Apr. 27, 2015, 11:07 AM), http://www.bloomberg.com/news/articles/2015-04-27/expensive-prison-skype-is-squeezing-out-in-person-visitation [https://perma.cc/44FP-X898].

the FCC to "encourage the deployment . . . of advanced telecommunications capability to all Americans."[21] The FCC relied on Section 706 in promulgating rules regarding "net neutrality," a principle of Internet governance that requires Internet service providers to handle Internet traffic similarly regardless of its source.[22] In *Verizon v. FCC*, the U.S. Court of Appeals for the D.C. Circuit largely agreed with the FCC's interpretation of Section 706.[23]

Section 222 of the Communications Act also provides the FCC with the authority to enforce privacy standards.[24] Section 222 requires "[e]very telecommunications carrier . . . to protect the confidentiality of proprietary information of, and relating to, . . . customers."[25] The FCC recently invoked its authority under Section 222 when requiring one Internet service provider to pay a substantial civil penalty and to implement data security safeguards in the aftermath of a data breach.[26]

II. DATA BREACHES AND SELLING TO THIRD PARTIES

By monitoring inmate communications, correctional contractors claim that their proprietary software can help correctional facilities analyze communications to "expose suspicious patterns."[27] While the government may have a legitimate interest in contracting with correctional contractors to perform these services, Part II will examine the type of data these contractors collect, and how sharing this data with private third parties—whether it be involuntarily through a data breach, or through a voluntary transaction—can undermine efforts to reduce recidivism rates.

A. What Correctional Contractors Collect

Correctional contractors collect a wide range of data. One correctional contractor, for example, collects the "date of birth, [and] social security

[21] 47 U.S.C. § 1302(a) (2012).

[22] Protecting and Promoting the Open Internet, 80 Fed. Reg. 19,738, 19,738 (Apr. 13, 2015) (to be codified at 47 C.F.R. pts. 1, 8, 20).

[23] 740 F.3d 623, 628 (D.C. Cir. 2014).

[24] 47 U.S.C. § 222 (2012).

[25] Id. § 222(a).

[26] Sam Pfeifle, FCC Fines AT&T $25m for Data Privacy Lapse; Who Will Be Next?, Int'l Ass'n Privacy Prof.: The Privacy Advisor (Apr. 9, 2015), https://iapp.org/news/a/fcc-fines-at-who-will-be-next/ [https://perma.cc/7QDY-5X5X].

[27] See, e.g., GTL Inmate Data Analysis, GTL, http://www.gtl.net/correctional-facility-services/investigative-solutions/data-analysis/ [https://perma.cc/M7FY-VJVW].

number" of its customers.[28] Another correctional contractor collects "[c]ontact information such as name, address, telephone number or email address," as well as "[c]redit/[d]ebit card information," and "the Internet Protocol (IP) address used to connect [a] computer or any internet-accessible device to the internet as well as login and password information."[29] Data pertaining to the content of communications is also collected, with one correctional contractor stating it reserves "the right to access, read, preserve, and disclose any information" sent through their emailing service,[30] as well as the "right to view, record, preserve, and disclose any information" contained in communications sent through its video-messaging service.[31]

Not only do correctional contractors collect this data about inmates, they also collect data about loved ones *outside* of correctional facilities. Indeed, correctional contractors are "able to identify the location of [a loved one's] mobile device," and may share "location information . . . with correctional facilities or other law enforcement personnel upon their request."[32] A third correctional contractor notes that they record "the websites . . . visit[ed] before or after" loved ones use their service.[33]

Collecting this type of sensitive and valuable data not only makes correctional contractors a target for hackers, it also means that these contractors have data that third parties are willing to pay for.[34] As Section II.B illustrates, although sharing this data with private third parties can undermine efforts to reduce recidivism rates, correctional contractors are currently free to do so.

---

[28] Privacy Policy, Securus, https://securustech.net/privacy [https://perma.cc/CP87-6JD7].

[29] Privacy Policy, JPay, http://www.jpay.com/LegalAgreementsOut.aspx [https://perma.cc/M8DM-FKCA].

[30] Email Terms of Service, JPay, http://www.jpay.com/LegalAgreementsOut.aspx [https://perma.cc/M8DM-FKCA].

[31] Video Visitation Terms of Service, JPay, http://www.jpay.com/LegalAgreementsOut.aspx [https://perma.cc/M8DM-FKCA].

[32] Global Tel*Link Corp., Privacy Statement 3, 5 (2015), http://www.gtl.net/wp-content/uploads/2015/04/GTL%20NET%20-%20Privacy%20Statement%20-%20Final%20-%20%2003-30-15.pdf [https://perma.cc/96LH-C8BT].

[33] Id. at 2.

[34] John W. Bagby, Balancing the Public Policy Drivers in the Tension Between Privacy and Security *in* 3 Cyber Crime: Concepts, Methodologies, Tools and Applications 1441, 1451 (Info. Res. Mgmt. Ass'n ed., 2012).

B. Current Privacy Policies Are Inadequate

Correctional contractors can share the data they collect about inmates and their loved ones quite freely. One correctional contractor's privacy policy states that "[w]e may use information collected from or about you . . . to send you . . . promotional materials from our marketing partners and other third parties; to deliver targeted display advertisements . . . [and] for any other business or marketing purposes that are not inconsistent with the terms of this Privacy Statement."[35] Another correctional contractor notes that they "do not sell, trade, or otherwise transfer to outside parties [customer's] personally identifiable information," *except* with "trusted third parties who assist [them] in . . . conducting [their] business."[36] Such language is opaque, and might be entirely circular if the correctional contractor's very "business" includes selling customer data in the first place. The appropriate policy question to ask, however, is not whether a specific correctional contractor is currently selling customer data, but whether correctional contractors should be in the position to freely do so in the first place. Current market conditions leave correctional contractors in such a position—with some correctional facilities beginning to replace in-person visitation hours with video-messaging services.[37]

This growing trend to replace in-person visitation hours with video-messaging services leaves inmates and their loved ones with little choice but to agree to the privacy policies offered by correctional contractors.[38] These families are often poverty-stricken, a fact raised in support of the FCC's objective to establish rate caps for telephone services.[39] Similar to how charging poverty-stricken families exorbitant prices for telephone services can increase their financial difficulties, requiring these same families to agree to the privacy policies currently offered by correctional contractors can create additional burdens on them in credit and labor

[35] Global Tel*Link Corp., supra note 32, at 4–5.

[36] General Terms and Conditions Including Privacy Policy, Product Terms and Conditions, and Mobile Terms and Conditions, Securus, https://securustech.net/terms-and-conditions#privacy [https://perma.cc/B6LX-VGXS].

[37] Stroud & Brunstein, supra note 20.

[38] Id.

[39] Ahiza Garcia, $14 a Minute? Pricey Prison Phone Calls Capped by FCC, CNN Money (Oct. 23, 2015, 9:54 AM), http://money.cnn.com/2015/10/23/news/fcc-prison-phone-call-rates/ [https://perma.cc/993Y-9RTF].

markets. These burdens can develop as a result of sharing either inaccurate or accurate data.

Data collected by correctional contractors can be inaccurate as a result of at least two issues. First, data might simply be incorrectly handled or labeled. This is of increased concern when it comes to data collected in jails, where inaccuracies may result in inmates being unjustly associated with crimes they have not been convicted of.

Second, *conclusions* drawn from underlying data can be inaccurate. This might result from the content of communications between inmates and their loved ones containing inaccuracies, or from questionable analysis performed after collection. One correctional contractor, for example, advertises that its product "enables correctional facilities to easily share with other facilities . . . to help find common phone numbers, expose larger gang networks, and generally provide the 'big picture' of the communications and interactions among inmates and their associates."[40] If an inaccurate conclusion is shared with third parties, it can unjustly stigmatize inmates in credit and labor markets. For example, inaccurately concluding that an inmate is associated with gang networks can make it more difficult for them to secure employment after their release.[41]

Consider the example of a job applicant in Arkansas who had incorrect data shared about her indicating that she was charged with the "intent to sell and manufacture methamphetamines."[42] Not only did this data result in her being denied employment, it prevented her from renting an apartment and even from obtaining credit to purchase a dishwashing machine.[43] Although the company that originally misreported this data corrected their records, the data had already been sold to other companies who "did not necessarily follow suit."[44] As more businesses turn to "data-driven" solutions, the market in which data is sold has become increasingly complex—with a correction of one company's records not necessarily resulting in a correction of the records held by any number of companies that have since obtained derivative copies of the underly-

[40] GTL Inmate Data Analysis, supra note 27.

[41] See Will Hobson, Police Gang Lists Can Have Life-Long Impacts and are Questioned by Legal Experts, Tampa Bay Times (Sept. 15, 2012, 7:08 PM), http://www.tampabay.com/news/publicsafety/crime/police-gang-lists-can-have-life-long-impacts-and-are-questioned-by-legal/1251855 [https://perma.cc/BAL7-J72G].

[42] Frank Pasquale, The Black Box Society 33 (2015) (internal quotation marks omitted).

[43] Id.

[44] Id.

ing data.[45] Sharing this type of sensitive data with employers, creditors, and landlords can leave former inmates unable to successfully integrate back into society.[46]

While inaccurate data presents one set of issues, additional issues arise even when accurate data is shared about a former inmate.[47] By creating an electronic record linking a former inmate with their incarceration, former inmates can find it increasingly difficult to distance themselves from the prior criminal acts for which they have already been punished.[48] This is of particular concern in light of the difficulties involved in unraveling the complex web of companies that sell and resell data. While some states have instituted "ban the box" laws that prohibit employers from inquiring into a job applicant's criminal record until later in the hiring process,[49] such laws are rendered ineffective where a simple Google search can reveal such information, or where private databases that cater to employers use such information as part of the database's underlying score of job applicants.[50] One must question the desirability of a system where former inmates are punished long after they have formally served their sentence, especially where the government has an interest in reducing the likelihood that such prolonged punishment occurs. In part as a response to this type of problem, the Court of Justice of the European Union held that E.U. citizens have a right to request that search engines remove links about them that are inaccurate or even "irrelevant."[51]

[45] See Andrew Guthrie Ferguson, Big Data and Predictive Reasonable Suspicion, 163 Univ. Pa. L. Rev. 327, 399–400 (2015).

[46] See Pasquale, supra note 42, at 22, 33–34 (describing how false claims regarding criminal history can negatively affect job applicants).

[47] See Jenny Roberts, Expunging America's Rap Sheet in the Information Age, 2015 Wis. L. Rev. 321, 341–42.

[48] See Laura Sullivan, Life After 'Life': Aging Inmates Struggling for Redemption, NPR (June 4, 2014), http://www.npr.org/2014/06/04/317055077/life-after-life-aging-inmates-struggle-for-redemption [https://perma.cc/X6SQ-4ZRU] ("Since he's been out, Huckleberry has found a couple of jobs, including one at a car dealership. But they fired him when they found out he's a felon.").

[49] Reid Wilson, Georgia the Latest State to 'Ban the Box' in Hiring Practices, Wash. Post (Feb. 24, 2015), https://www.washingtonpost.com/blogs/govbeat/wp/2015/02/24/georgia-the-latest-state-to-ban-the-box-in-hiring-practices/ [https://perma.cc/QGH2-AF9W].

[50] See Stephanie Clifford & Jessica Silver-Greenberg, Retailers Track Employee Thefts in Vast Databases, N.Y. Times (Apr. 2, 2013), http://www.nytimes.com/2013/04/03/business/retailers-use-databases-to-track-worker-thefts.html [https://perma.cc/VEK9-UKCQ].

[51] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014), http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text&pageIn

This "right to be forgotten" requires search engines to "assess deletion requests on a case-by-case basis" to determine if a given link must be removed under E.U. law.[52] While such a regime might prevent a former inmate from being continually denied credit and employment opportunities, the First Amendment likely prohibits U.S courts from finding a similar right.[53] The FCC, however, is able to limit a correctional contractor's ability to *sell* this data as a precondition to being awarded a government contract. Section II.C will outline how the FCC should establish such a precondition.

C. How the FCC Can Protect Privacy

Just as the FCC established boundaries within which companies may contract with correctional facilities to provide telephone services, the FCC should establish similar boundaries regarding Internet services. In addition to establishing rate caps for Internet services, the FCC should regulate these services on two additional fronts.

First, the FCC should prohibit correctional contractors from selling the data they collect from inmates and their loved ones to private third parties. While it is appropriate to require inmates and their loved ones to agree to a reasonable degree of monitoring by law enforcement to ensure that Internet services are not used for nefarious communications, selling this data to private third parties unnecessarily undermines efforts to reduce recidivism rates by placing substantial burdens on former inmates in credit and labor markets. Regardless of the extent to which selling customer data is already a major component of a correctional contractor's business model, the FCC should act now to curtail it. While selling customer data may be a valuable perk of providing Internet services within correctional facilities, it is a perk that must be trumped by efforts to successfully integrate former inmates back into society.

Second, the FCC should make clear that correctional contractors will be held financially liable for data breaches. Just as selling data can place substantial burdens on former inmates in credit and labor markets, these same burdens can result where data is shared as a result of a data breach.

---

dex=0&part=1&mode=DOC&docid=152065&occ=first&dir&cid=437838 [https://perma.cc/4SL7-H3LJ].

[52] European Comm'n, Factsheet on the "Right to be Forgotten" Ruling (C-131/12), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf [https://perma.cc/9KTZ-RXNZ].

[53] Jeffrey Rosen, The Right to be Forgotten, 64 Stan. L. Rev. Online 88, 88 (2012).

Earlier in 2015 the FCC entered into a consent agreement with one Internet service provider—AT&T—after customers' social security numbers were leaked.[54] Under the consent agreement, AT&T was required to "pay a civil penalty of $25,000,000 and develop and implement a compliance plan to . . . protect consumers against similar data breaches in the future."[55] The FCC should make it clear that correctional contractors would face similar liability in the wake of a data breach.

By making it clear that correctional contractors will be held liable in the wake of a data breach, the FCC can place correctional contractors on notice of the significant impact that the data they collect can have on society's interest in reducing recidivism rates.[56] As the original collectors of the data, placing liability on correctional contractors is appropriate in light of the difficulties involved in tracing how data is repackaged and shared once it is originally leaked. By establishing clear liability guidelines, the FCC can provide correctional contractors with an incentive to appropriately protect the sensitive data they collect, and ensure that the costs of a data breach are not disproportionately placed on former inmates and their loved ones.

CONCLUSION

While correctional contractors provide a valuable service that can help reduce recidivism rates, the privacy policies they currently offer undermine that goal. Sharing sensitive data about inmates and their loved ones—whether it be involuntarily through a data breach, or through a voluntary transaction—illustrates one way these privacy policies fall short. The FCC can correct this issue by prohibiting correctional contractors from selling the data they collect to private third parties, and by establishing clear liability guidelines for data breaches.

[54] Pfeifle, supra note 26.

[55] AT&T Servs., Inc., 30 FCC Rcd. 2808 (2015).

[56] See, e.g., Danielle Keats Citron, Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age, 80 S. Cal. L. Rev. 241, 264–67 (2007).