Docket:	A.18-07-011 and A.18-07-012
Exhibit Number:	Cal Advocates-
Commissioner:	C. Rechtschaffen
Admin. Law Judge:	K. J. Bemesderfer
Cal Advocates Project Mgr.:	Shelly Lyser
Cal Advocates Expert Witness:	Kristina Donnelly

Public Advocates Office

California Public Utilities Commission

Public Advocates Office Testimony on Privacy for the Proposed Transfer of Control of Sprint to T-Mobile

- PUBLIC -

San Francisco, California
January 7, 2019

MEMORANDUM

This report was prepared by Kristina Donnelly of the Public Advocates Office at the California Public Utilities Commission ("Public Advocates Office") under the general supervision of Program & Project Supervisor, Shelly Lyser. Attachment A to this testimony is a statement of qualifications from Kristina Donnelly. The Public Advocates Office is represented in this proceeding by legal counsel, Travis Foss.

This testimony is comprised of the following chapters:

Chapter	Description
I	**Third Party Access to Customer Data**: Describes and compares the customer data privacy and security risks posed by T-Mobile's and Sprint's third-party relationships.
II	**Children and Data Collection:** Describes and compares T-Mobile's and Sprint's approach to managing data and information collected from devices belonging to children.

CONTENTS

ATTACHMENTS

Page

SUMMARY

This testimony summarizes the potential impact of the proposed transaction on consumer privacy and data security. Although the results of this analysis suggest that both companies engage in practices that put customer privacy and data security at risk, the overall risk to customer privacy and data security would likely increase for Sprint customers following a merger with T-Mobile.

Should the Commission fail to deny approval of the Joint Applicant's request, the Commission should develop mitigating conditions that are enforceable, measurable, able to be tracked and monitored on an on-going basis that address the following areas:

- New T-Mobile should create an inventory of all third-party suppliers and subcontractors[1] who have or will have access to New T-Mobile customer data. New T-Mobile should use this inventory to conduct regular, periodic reviews of suppliers' and subcontractors' data security and risk management policies and programs. New T-Mobile should require third parties notify and receive approval from New T-Mobile when providing subcontractors access to customer data.
- New T-Mobile should make third party risk management is a company-wide priority. New T-Mobile should ensure the Board of Directors and other senior leadership receive periodic updates from staff about the status of the company's third-party risk management programs. New T-Mobile should require staff to report to the board and senior leadership whenever a data breach occurs.
- New T-Mobile should require third parties to notify New T-Mobile staff within 24 hours of a data breach or suspected breach, whether the breach originates with the third party or their subcontractor. Supplier contracts should clearly state how suppliers must notify New T-Mobile in the event of a data breach and should require suppliers provide periodic reports and updates describing the breach investigation and all corrective or remedial actions taken.
- New T-Mobile should allow customers to identify devices that belong to children and establish a program that would give primary account holders increased control over the data generated by devices that belong to children. This increased control should include the ability for the primary account holder to control what data are collected and to have New T-Mobile delete the data that are collected. In addition, New T-Mobile should not collect or store any information from these devices, beyond what is

[1] In this document, I use "subcontractor," "third party subcontractor," and "Nth party" interchangeably to refer to a third-party supplier's own third-party relationships.

necessary to provide service. New T-Mobile should also not use the data, even if the data are de-identified, for any purpose other than providing service to that device. New T-Mobile should automatically preclude children's devices from inclusion in any interest-based advertising program, even if other types of customers must "opt-out."

- New T-Mobile should employ an independent consultant to conduct a customer satisfaction survey on their respective company's data privacy policies including customer notice and understanding of those privacy standards, customer ability and accessibility to opt-in/opt-out of carriers' data collection, and customer notification and recourse when data are compromised or breached. The independent consultant should work with the Public Advocates Office and other consumer groups that are parties in this proceeding on the survey methodology and design, and should share the results of the survey with them and the Commission.

I. THIRD PARTY ACCESS TO CUSTOMER DATA

Third parties provide telecommunications companies a variety of services – including billing, network analysis, and, increasingly, advertising.[2] Many of these services require third parties to access customer information, whether in whole or in part, identifiable or "deidentified".[3] However, third party data sharing agreements open companies up to an increased risk of data breaches; a 2014 study estimated that, in the retail sector, one-third of all data breaches originated with these third parties.[4] Another report published in November 2018 shows that, of the US-based companies surveyed, 61 percent experienced a third party data breach in 2018, an increase from 56 percent of respondents in 2017 and 49 percent of respondents in 2016.[5]

All the major wireless carriers, including Sprint and T-Mobile, are at risk from data breaches that originated with their third-party partners, and both companies name third party data breaches as a business risk in their annual 10-K filings with the Securities and Exchange Commission.[6, 7] Both Sprint and T-Mobile have already experienced third-party data breaches involving customer data. Arguably one of the most high-profile examples is the Experian data breach that occurred in 2015, where hackers stole the social security numbers and personal

---

[2] Kaye, Kate. 2017. "Startups Put Mobile Carrier Data Into Advertiser Hands." AdAge, March 9, 2017. Accessed: December 13, 2018. https://adage.com/article/dataworks/startups-put-mobile-carrier-data-advertiser-hands/308198/.

[3] As defined in the California Consumer Privacy Act of 2018 (SB 1211), "deidentified" means "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer."

[4] Stevens, Melissa. 2014. "New Research Shows One Third of Retail Breaches Originated from Third-Party Vulnerabilities." BitSight. Accessed: December 13, 2018. https://www.bitsighttech.com/press-releases/news/new-research-shows-one-third-of-retail-breaches-originated-from-third-party-vulnerabilities.

[5] Ponemon Institute LLC. 2018. "Data Risk in the Third-Party Ecosystem Third Annual Report." Research Report Sponsored by Opus. Accessed: December 13, 2018. https://www.opus.com/ponemon/.

[6] Sprint Corporation. 2018. "Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934." SEC filing for the fiscal year ended March 31, 2018. Pp. 22-23. Accessed: December 13, 2018. http://investors.sprint.com/financials/default.aspx.

[7] T-Mobile US Inc. 2018. "Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934." SEC filing for the fiscal year ended December 31, 2017. Pp. 11-12. Accessed: December 13, 2018. https://investor.t-mobile.com/financial-performance/sec-filings/default.aspx.

information of 15 million T-Mobile customers.[8] Another recent example began to be widely reported on in May 2018, after documents[9] and articles[10] revealed that U.S. wireless carriers had sold real-time customer geolocation information to law enforcement agencies through Securus Technologies,[11] which was found to be providing access to this information without obtaining customer consent or reviewing a court order. Securus had originally purchased the geolocation information from 3Cinteractive, which had obtained it from a California-based company, LocationSmart, which had in turn purchased it from the largest wireless carriers in the United States, including AT&T, Verizon, T-Mobile, Sprint, US Cellular.[12, 13] In June 2018, Verizon, AT&T, T-Mobile, and Sprint announced that they would terminate their location-sharing agreements with Securus and LocationSmart;[14] however, LocationSmart's website still claims that it has "direct connections to Tier 1 and Tier 2 wireless carriers" and can "deliver access to more than 400 million mobile devices across the U.S. and Canada."[15]

Because carriers lack direct access to and control of third-party data security policies and practices, they must manage this risk through their own risk management policies and practices, as well as through contracts with third parties. However, these methods can vary widely in their

---

[8] Krebs, Brian. 2015. "At Experian, Security Attrition Amid Acquisitions." Krebs on Security (blog). October 8, 2015. Accessed: December 13, 2018. https://krebsonsecurity.com/2015/10/at-experian-security-attrition-amid-acquisitions/.

[9] Ron Wyden. 2018. "Letter from Senator Ron Wyden to Chairman of the FCC Ajit Pai," May 8, 2018. Accessed: December 13, 2018. https://www.wyden.senate.gov/download/wyden-letter-to-fcc-on-securus-location-tracking.

[10] Jennifer Valentino-DeVries. 2018. "Service Meant to Monitor Inmates' Calls Could Track You, Too." The New York Times, May 10, 2018. Accessed: December 13, 2018. https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html.

[11] Securus Technologies provides communications and technology services to correctional facilities nationwide. According to its website, Securus Technologies provides phone, video, and other services to approximately 70 facilities in California (See: https://securustech.net/facilities-we-serve).

[12] Whittaker, Zack. 2018. "US Cell Carriers Are Selling Access to Your Real-Time Phone Location Data." ZDNet. May 14, 2018. Accessed: December 13, 2018. https://www.zdnet.com/article/us-cell-carriers-selling-access-to-real-time-location-data/.

[13] Both LocationSmart and Securus have had other security breaches; for more information, please see: https://krebsonsecurity.com/2018/05/mobile-giants-please-dont-share-the-where/#more-43895 and https://www.ibtimes.com/securus-technologies-rogue-employee-not-hacker-exposed-70-million-inmate-calls-2181819 and https://motherboard.vice.com/en_us/article/gykgv9/securus-phone-tracking-company-hacked

[14] "AT&T, Sprint, Verizon to Stop Sharing Customer Location Data With Third Parties." 2018. Krebs on Security (blog). June 19, 2018. Accessed: December 20, 2018. https://krebsonsecurity.com/2018/06/verizon-to-stop-sharing-customer-location-data-with-third-parties/.

[15] LocationSmart. 2018. "Carrier Network Location Collateral - Secure and Trusted Location-as-a-Service." 2018. Accessed: December 20, 2018. https://www.locationsmart.com/resources/carrier-network-location.

scope, efficacy, and execution. Therefore, I examine both Sprint's and T-Mobile's third-party policies and practices to determine whether both companies employ industry best practices when they provide third parties access to their customers' data and information. To do this, I rely on recommendations from an annual report published by the Ponemon Institute[16] that summarizes the results of a survey designed to assess data risks in the third party "ecosystem," a term the report uses to describe direct and indirect relationships that companies have with third parties as well as their respective third parties (called "Nth parties").[17, 18] The third annual report, published in November 2018, examines how "high performing" organizations – defined as those that have not experienced a third party data breach in at least the past 12 months, if ever – differ from other respondents that had experienced a breach. Based in part on this analysis, the report makes several recommendations designed to help companies better manage third party ecosystem risks, which I use to evaluate T-Mobile's and Sprint's third-party policies and practices. Specifically, I review whether and how well both T-Mobile and Sprint implement the following three recommendations:

- Evaluate the data safeguards, and security policies, practices, and procedures of all third parties before engaging them and periodically thereafter.
- Ensure that managing the company's outsourced relationship risk is a company priority.
- Require third-parties to notify the company in the event of a data breach, whether the breach originates with the third party or their subcontractor.

A. Thoroughly evaluate all third parties before engaging them and periodically thereafter.

Companies with effective third-party risk management programs evaluate and monitor the data safeguards, and security policies, practices, and procedures of both suppliers and supplier subcontractors. According to the Ponemon Report, 50 percent of respondents from "high performing" companies,[19] compared to 31 percent of respondents from other companies,

---

[16] The Ponemon Institute conducts independent research on privacy, data protection, and information security policy.

[17] Ponemon Institute LLC. 2018. "Data Risk in the Third-Party Ecosystem Third Annual Report." Research Report Sponsored by Opus. Accessed: December 13, 2018. https://www.opus.com/ponemon/.

[18] Note that, in this document, I use "third-parties" and "suppliers" interchangeably. I also use the terms "third party subcontractor," "supplier subcontractor," and "Nth party" interchangeably.

[19] As described in the introductory section, the Ponemon Report defines "high performing" organizations as those that have not experienced a third-party data breach in at least the past 12 months, if ever.

evaluate the security and privacy practices of all third parties before engaging them. Respondents from high performing companies also reported higher confidence that their third parties' data safeguards and security policies and procedures are sufficient to prevent a data breach.

Therefore, I examine T-Mobile's and Sprint's policies and practices in order to determine whether T-Mobile and Sprint evaluate third parties before forming a relationship with them, and whether they conduct additional, periodic evaluations in order to ensure the supplier is adequately managing both existing and emerging risks.

1. T-Mobile's new process for evaluating third-party data risks has some gaps.

T-Mobile relies on a few different documents to implement the company's third-party evaluation process:

- **TISS-610:** T-Mobile outlines its third-party risk management process in "TISS-610 Enterprise Third-Party (Supplier) Information Security Standard" (TISS-610), which went into effect during the first week of December 2018.[20, 21] TISS-610 applies to all suppliers, including those that access, host, retain, process, or transmit non-public T-Mobile information.
- **Exhibit B:** T-Mobile also relies on the suppliers' contractual terms and conditions to ensure suppliers' data security practices are evaluated and monitored when suppliers have access to T-Mobile's confidential information.[22] Although T-Mobile tailors the specific terms and conditions to each individual supplier, T-Mobile provided a copy of a general template of this contractual language; T-Mobile (and therefore this testimony) refers to this template as "Exhibit B."[23]
- **Cyber Assessment Questionnaire:** TISS-610 references a "Cyber Assessment Questionnaire," a copy of which T-Mobile provided to the Public Advocates

[20] Exhibit D-1: T-Mobile Supplemental Response to Public Advocates Office DR 4-22

[21] A copy of TISS-610 is provided in Exhibit D-2. TISS-610 replaced the similarly-named "TRS-610 Enterprise Third-Party (Supplier) Risk Management Standard" in the first week of December 2018. As of January 2, 2019, TRS-610 was still available on T-Mobile's website (See: https://www.t-mobile.com/our-story/working-together/suppliers/supplier-code-of-conduct.)

[22] Exhibit D-3: T-Mobile Response to Public Advocates Office DR 4-26

[23] Exhibit D-4: T-Mobile Response to Public Advocates Office DR 4-26 CONFIDENTIAL Attachment "TMUS-CPUC-PA-13000073(Highly Confidential - Attorneys Eyes Only).PDF"

Office.[24] The Cyber Assessment Questionnaire went into effect in early October 2018.[25]

TISS-610 does not clearly indicate when T-Mobile conducts in-depth security reviews of all new suppliers, prior to formalizing a relationship with them. Section 1 of TISS-610 states that T-Mobile completes an "Enterprise (Supplier) Risk Management Program (ESRAP) intake" for all suppliers, and the results of the intake *may* trigger a "Cyber Assessment." However, TISS-610 does not describe what information T-Mobile collects during the ESRAP intake or what information would trigger the Cyber Assessment. The "Cyber Assessment Questionnaire" **[BEGIN T-MOBILE CONFIDENTIAL]** [redacted] **[END T-MOBILE CONFIDENTIAL]**

In response to a Public Advocates Office Data Request, T-Mobile stated, "T-Mobile Third Party Risk Management ("TPRM") processes utilize an objective framework to rank the findings and risk information gleaned from third-party due diligence reviews and assessments. Risk information is escalated, where warranted, for evaluation and decision as to whether to approve, reject, or condition a supplier engagement."[27] Again, T-Mobile did not provide any description of the "objective framework" or the ranking methodology, and did not indicate what specific documents comprise the "due diligence reviews and assessments." T-Mobile also did not indicate to whom the risk information is escalated, when escalation is warranted, or how conditions for supplier engagement are determined and approved. Since these details are very relevant to supplier risk management, I would expect to see them described in TISS-610 or another internal document, yet they are not described in any of the documents T-Mobile submitted to the Public Advocates Office.

Exhibit B **[BEGIN T-MOBILE CONFIDENTIAL]** [redacted]

---

[24] Exhibit D-5: T-Mobile Supplemental Response to Public Advocates Office DR 4-22 CONFIDENTIAL Attachment "TMUS-CPUC-PA-00005641.Confidential.pdf"

[25] The Cyber Assessment Questionnaire replaces the "SRM Questionnaire" that is described in the now-defunct TRS-610. (See: Exhibit D-1: Supplemental Response to Public Advocates Office DR 4- 22)

[26] Exhibit D-5: T-Mobile Supplemental Response to Public Advocates Office DR 4-22 CONFIDENTIAL Attachment "TMUS-CPUC-PA-00005641.Confidential.pdf"

[27] Exhibit D-3: T-Mobile Response to Public Advocates Office DR 4-26

[redacted] **[END T-MOBILE CONFIDENTIAL]**

T-Mobile's Cyber Assessment Questionnaire **[BEGIN T-MOBILE CONFIDENTIAL]** [redacted] **[END T-MOBILE CONFIDENTIAL]**

---

28 Although the version of Exhibit B that Public Advocates Office received from T-Mobile on December 4, 2018 **[BEGIN T-MOBILE CONFIDENTIAL]** [redacted] **[END T-MOBILE CONFIDENTIAL]**

Exhibit B **[BEGIN T-MOBILE CONFIDENTIAL]** [redacted] **[END T-MOBILE CONFIDENTIAL]**

2. Sprint's third-party review process also contains some important gaps.

The process Sprint uses to evaluate its third-party data sharing agreements **[BEGIN SPRINT CONFIDENTIAL]** [redacted]

[29] Exhibit D-6: Public Advocates Office DR 4-4

[30] Exhibit D-7: Sprint Response to Public Advocates Office DR 4-4 CONFIDENTIAL Attachment "Cal PA DR 004 - DR 4-4(a) - Outside Resource Committee.pdf"

[redacted] **[END SPRINT CONFIDENTIAL]**

B. Managing the company's outsourced relationship risk should be a company priority.

Making third-party risk management a company-wide priority begins with the Board of Directors and includes senior-level staff. Companies that cite managing supplier risk as a company priority are more likely to implement effective risk management policies and programs. According to the Ponemon Report, 60 percent of respondents from high performing companies[32] say that managing outsourced relationship risk is a priority, compared to 33 percent of respondents from other companies. Fifty-three percent of respondents from high performing companies, compared to 25 percent of respondents from other companies, say they regularly report to the board of directors on the effectiveness of the third-party management program and potential risks to the organization. Not only does company-wide prioritization send a signal to employees about the importance of this risk, it also provides a mechanism for ensuring the company allocates sufficient resources to manage it; for example, according to the Ponemon

---

[31] Exhibit D-8: Sprint Response to Public Advocates Office DR 4-4CONFIDENTIAL Attachment "Cal PA DR 004 - DR 4-4(a) - Model privacy language.pdf"

[32] As described in the introductory section, the Ponemon Report defines "high performing" organizations as those that have not experienced a third-party data breach in at least the past 12 months, if ever.

Report, 60 percent of respondents from high performing companies, compared to 15 percent of respondents from other companies, say they allocate sufficient resources to managing outsourced relationships. In this section, I examine whether third-party data risk management is a company-wide priority for both T-Mobile and Sprint.

1. T-Mobile should explicitly make supplier risk management a company-wide priority.

The documents and responses that T-Mobile submitted to the Public Advocates Office do not indicate whether supplier risk management is a company-wide priority. In addition, neither TISS-610 nor any other response or document received from T-Mobile specify whether the company's senior leadership or boards of directors receive periodic updates regarding T-Mobile's third-party risk management program.

Through an Internet search, I found a T-Mobile webpage that describes the Board of Director's risk management responsibilities and activities.[33], [34] While this webpage does not clearly state whether the risk management program it describes includes supplier risk management, it seems reasonable to assume that it might. According to this webpage, T-Mobile has an "Information Security and Privacy Council" that is supported by the Senior Vice President of Digital Security (who serves as the Chief Information Security Officer), and the Vice President, Chief Privacy Officer. The website says that the Council oversees the "strategic governance and prioritization of the Company's information security and privacy initiatives." While these public-facing documents do not state whether the Council oversees third-party information security and privacy, the fact that the Council is comprised of senior leadership is a good indicator of a company-wide commitment to information security and privacy. However, without the details that we would have expected T-Mobile to provide in response to our request to "describe how T-Mobile assesses, manages, and monitors risks posed by third party access to customer data,"[35] and since the Council is not mentioned in any of the documents we received

[33] T-Mobile. "Our Board & Governance: Risk Management." T-Mobile's 2018 Digital Proxy Statement. Accessed: December 12, 2018. https://explore.t-mobile.com/2018-proxy-statement/board-and-governance/risk-management

[34] Note that we examined T-Mobile's Digital Proxy Statement, and not the full statement, because the download link on the 2018 Digital Proxy page (https://explore.t-mobile.com/2018-proxy-statement) was broken as of January 2, 2019. (See error message here: https://investor.t-mobile.com/Cache/1500109983.PDF?O=PDF&T=&Y=&D=&FID=1500109983&iid=4091145).

[35] Exhibit D-3: Public Advocates Office DR 004, Question 26.

from T-Mobile, we can only speculate about either the Council's or the Board's involvement in and oversight of T-Mobile's third-party risk management process.

2. Sprint should explicitly make supplier risk management a company-wide priority.

None of the documents or responses received from Sprint indicate whether the Board of Directors or senior management are actively engaged in the company's third-party risk management process, or whether they receive regular updates about the program from staff.

As with T-Mobile, through an Internet search, I found and reviewed the publicly available guidelines that describe the roles and responsibilities of Sprint's Board of Directors.[36] Sprint's "Corporate Governance Guidelines" does not specifically mention supplier risk management, customer privacy, or information security. The Guidelines do say that the board is responsible for reviewing and approving the company's plans, strategies, and other polies, and is responsible for "assessing Sprint's material risks and business resiliency." The Board's Audit Committee Charter states that the Audit Committee will "review guidelines and policies with respect to risk assessment and risk management" and will "annually report to the Board regarding Sprint's Enterprise Risk Management Program." While it would make sense for supplier risk to be within the Committee's purview, no document we received or reviewed make that explicit. As with T-Mobile, the fact that Sprint does not highlight its third-party risk management process or activities indicates that third-party risk management might not be a priority for Sprint's Board of Directors.

C. Third-parties should be required to provide notification in the event of a data breach.

The Ponemon survey found that most respondents are not confident they would receive notification in the event of a third party or Nth party data breach if it involved their company's sensitive and confidential information; 29 percent of respondents were confident their suppliers would notify them in the event of a data breach and 12 percent were confident suppliers would notify them in the event of an Nth party data breach. Since companies can only respond to a data

[36] Sprint. 2018. "Sprint Corporation - Corporate Governance." Accessed: December 13, 2018. http://investors.sprint.com/corporate-governance/default.aspx.

breach if they know that one has occurred, I also examine T-Mobile's and Sprint's third-party data breach notification polices.

1. T-Mobile's third-party data breach notification requirements should go further

While the documents we reviewed show that T-Mobile **[BEGIN T-MOBILE CONFIDENTIAL]** [redacted] **[END T-MOBILE CONFIDENTIAL]**, T-Mobile's notification requirements are less specific than those outlined by Sprint.

TISS-610 requires suppliers to "have the capacity" to notify T-Mobile of any security breach; however, TISS-610 does not specifically require notification, nor does it specify what information the supplier must report, to whom, or when. TISS-610 also does not outline what security actions suppliers must take in the event of a data breach. Instead, Section 4.2 of TISS-610 focuses on controlling how the breach is communicated publicly:

> "Supplier must have the capacity to immediately notify T-Mobile of any security breach and must assist T-Mobile in investigating the security breach in accordance with terms of an approved contract, work order, or master service agreement. Supplier must have technical, administrative and physical security measures in-place so that vulnerabilities are disclosed responsibly, and that information about a security breach impacting T-Mobile information is not disclosed to the public until authorized to do so by T-Mobile." (emphasis in the original)

[BEGIN T-MOBILE CONFIDENTIAL] [redacted]

[redacted] **[END T-MOBILE CONFIDENTIAL]**

2. Sprint has a relatively more detailed and specific policy for third parties to follow in the event of a data breach

Sprint provided the Public Advocates Office with a model of the general privacy and data security requirements that Sprint includes in contracts with third parties when those agreements include data sharing.[37] This document **[BEGIN SPRINT CONFIDENTIAL]** [redacted] **[END SPRINT CONFIDENTIAL]**

D. Conclusions

While T-Mobile does have an established third-party review process, the documentation provided to the Public Advocates Office suggest that the process likely contains some important gaps. TISS-610 states that it conducts a "Cyber Assessment" when triggered by an ESRAP intake; however, neither TISS-610 nor the **[BEGIN T-MOBILE CONFIDENTIAL]** [redacted] **[END T-MOBILE CONFIDENTIAL]** contain sufficient information to determine what conditions would trigger the full assessment. **[BEGIN T-MOBILE CONFIDENTIAL]** [redacted] **[END T-MOBILE CONFIDENTIAL]** While T-Mobile staff may be trained or otherwise informed about how to implement the company's third part risk management process, T-Mobile does not include or describe them in any of the documents or responses provided to the Public Advocates Office.

[37] Exhibit D-8: Sprint Response to Public Advocates Office DR 4-4 CONFIDENTIAL Attachment "Cal PA DR 004 - DR 4-4(a) - Model privacy language.pdf"

In addition, while T-Mobile did not indicate whether or to what extent supplier risk management and data privacy and security is a company-wide priority, our review of T-Mobile's 2018 Digital Proxy Statement suggests that the board of directors may not be as engaged in these risks as recent research suggests they should be. Finally, **[BEGIN T-MOBILE CONFIDENTIAL]** [redacted] **[END T-MOBILE CONFIDENTIAL]**

Sprint's third-party risk management review process is relatively more robust than T-Mobile's, but it also contains some important gaps. Instead of relying on a variety of processes, forms, rankings, and frameworks, some of which appear to be unspecified, **[BEGIN SPRINT CONFIDENTIAL]** [redacted] **[END SPRINT CONFIDENTIAL]**

Therefore, should the Commission fail to deny approval of the Joint Applicant's request, the Commission should develop mitigating conditions that are enforceable, measurable, able to be tracked and monitored on an on-going basis that address the following areas:

- New T-Mobile should create an inventory of all third-party suppliers and subcontractors who have or will have access to New T-Mobile customer data. New T-Mobile should use this inventory to conduct regular, periodic reviews of suppliers' and subcontractors' data security and risk management policies and programs. New T-Mobile should require third parties notify and receive approval from New T-Mobile when providing subcontractors access to customer data.
- New T-Mobile should make third party risk management is a company-wide priority. New T-Mobile should ensure the Board of Directors and other senior leadership receive periodic updates from staff about the status of the company's third-party risk

management programs. New T-Mobile should require staff to report to the board and senior leadership whenever a data breach occurs.

- New T-Mobile should require third parties to notify New T-Mobile staff within 24 hours of a data breach or suspected breach, whether the breach originates with the third party or their subcontractor. Supplier contracts should clearly state how suppliers must notify New T-Mobile in the event of a data breach and should require suppliers provide periodic reports and updates describing the breach investigation and all corrective or remedial actions taken.

II. CHILDREN AND DATA COLLECTION

Children of all ages use cell phones, whether it is a phone that belongs to them exclusively, or to a parent, relative, or other adult.[38] A Pew Research report from 2009 showed that, for children under the age of 18, 43 percent had first received a mobile device when they were under 13.[39] The Pew report also found that the average age a child received their first device was nearly 13; however, the report also suggested that the average age at which children received their first device was decreasing over time, which is supported by at least one recent estimate from 2016 that suggests the age has dropped to around 10 years old.[40, 41]

All children, especially the very young, are much more vulnerable to data breaches and predatory marketing than adults.[42] Children are also frequent targets for fraud because their credit history is clean and infrequently monitored; Experian estimates that, by the time children today turn 18, approximately one-quarter will have experienced identity fraud or theft.[43] As a result, children require additional, increased protections when they use Internet-connected devices. This is particularly important given how long-lived the consequences may be, particularly for today's generation of children:

> "The digital dossiers that may be compiled about children from a young age may have long-term consequences once a child reaches adulthood. The ubiquitous nature of IOT

---

[38] For the purposes of this report, unless otherwise specified, "children" refers to individuals who are under the age of 13. Although adolescents can be just as vulnerable as children under the age of 13, we limit this chapter to children under the age of 13 as this is the limit that is used in federal regulations like COPPA. (See: Montgomery, Kathryn C., Jeff Chester, and Tijana Milosevic. 2017. "Children's Privacy in the Big Data Era: Research Opportunities." Pediatrics 140 (Supplement 2): S117–21. https://doi.org/10.1542/peds.2016-1758O.)

[39] Lenhart, Amanda. 2010. "Is the Age at Which Kids Get Cell Phones Getting Younger?" Pew Research Center. December 1, 2010. Accessed: December 12, 2018. http://www.pewinternet.org/2010/12/01/is-the-age-at-which-kids-get-cell-phones-getting-younger/.

[40] Donovan, Jay. 2016. "The Average Age for a Child Getting Their First Smartphone Is Now 10.3 Years." TechCrunch, May 19, 2016. Accessed: December 12, 2018. http://social.techcrunch.com/2016/05/19/the-average-age-for-a-child-getting-their-first-smartphone-is-now-10-3-years/.

[41] Influence Central. 2016. "Kids & Tech: The Evolution of Today's Digital Natives." Accessed: December 12, 2018. https://web.archive.org/web/20181211155244/http://influence-central.com/kids-tech-the-evolution-of-todays-digital-natives.

[42] Montgomery, Kathryn C., Jeff Chester, and Tijana Milosevic. 2017. "Children's Privacy in the Big Data Era: Research Opportunities." Pediatrics 140 (Supplement 2): S117–21. https://doi.org/10.1542/peds.2016-1758O.

[43] Experian. 2018. "Identity Theft Statistics." March 15, 2018. Accessed: October 1, 2018. https://www.experian.com/blogs/ask-experian/identity-theft-statistics/.

toys, social networks, and various devices that minors use to access the Internet ensure that children begin leaving digital footprints much earlier than previous generations."[44]

Because wireless companies are in a unique position to collect, store, and use customer data, devices belonging to children warrant increased protections and limitations on data sharing, data collection, and marketing. Federal law protects children's online privacy and safety through the Children's Online Privacy Protection Act (COPPA).[45] COPPA has multiple rules that apply to companies that provide "online services." COPPA provides specific rights to guardians with respect to the personal information collected from their children. According to COPPA, companies must:

- give guardians a way to review the personal information collected from their child;
- give guardians a way to revoke their consent and refuse the further use or collection of personal information from their child; and
- delete a child's personal information upon request from the guardian.

It is important to note that COPPA rules only apply when companies have "actual knowledge" that they collect personal information from children under 13.[46]

According to 2017 estimates from the KIDS COUNT Data Center, approximately 9.6 million people under the age of 18 and 6.5 million under the age of 13 live in California.[47] Although we do not know how many of these children are provided their own mobile phone, the research cited here suggests the number could be in the millions.

Both T-Mobile and Sprint have special sections of their privacy policies that detail how the policy applies to children.[48] Below, I review the content of these sections to determine how well T-Mobile and Sprint protect this sensitive category of customers.

---

[44] Elvy, Stacy-Ann. 2017. "Paying for Privacy and the Personal Data Economy." Columbia Law Review 117 (6): 92.

[45] 16 CFR 312

[46] 16 CFR 312.2

[47] KIDS COUNT Data Center. 2018. "Child Population by Single Age." August. Accessed: December 27, 2018. https://datacenter.kidscount.org/data/Tables/100-child-population-by-single-age.

[48] Exhibit D-9 and D-10: Complete versions of T-Mobile's and Sprint's current privacy policies.

A. Sprint Gives Primary Account Holders Special Control Over the Data Generated by Devices Provided to Children; However, This Control Is Only Available to a Very Small Subset of Customers

Under the heading "Children," Sprint's Privacy Policy states the following:[49]

> You must be 18 or otherwise have legal capacity to subscribe to Sprint services. Nevertheless, as part of the Unlimited, My Way Student Promotion, a parent or legal guardian may provide a Sprint device to a child under the age of 13. Sprint takes steps to minimize the data it collects from Sprint applications on the device and provides parents resources to control the information children can share with other parties. In some instances, a parent may be able to review or request deletion of the personal information collected from a child's device, or take steps to prevent further collection of such information. If you have any questions about Sprint's policies for student phones or about how to control the information collected on them from users under 13, or if you wish to correct or delete any personal information provided to Sprint on a student phone used by a child under 13, you can contact us using the contact information below. You may also control the content your child may access by logging into sprint.com/manage, and reviewing the My Preferences tab.[50]

The second sentence of this paragraph describes the "Unlimited, My Way Student Promotion" as a way for parents or guardians to provide a device to a child.[51] However, as written, it is unclear whether the subsequent terms of this paragraph apply to *any* device provided to a child under the age of 13, or *only* to devices that are provided as part of the "Unlimited, My Way Student Promotion." In response to inquiry from the Public Advocates Office, Sprint responded that the conditions outlined in the "Children" section of their Privacy Policy do *not* apply *only* to devices that are provided to children under the "Unlimited, My Way Student Promotion."[52] However, Sprint also stated that: "The 'Unlimited, My Way Student Promotion' was the only Sprint promotion directed to parents of children under the age of 13, other than the Pokémon GO Mobile Trainer Rewards program. *Sprint does not have knowledge of, and will not*

---

[49] Exhibit D-10: Sprint. 2017. Sprint Corporation Privacy Policy. March 29th. Accessed: December 13, 2018. https://www.sprint.com/en/legal/sprint-corporation-privacy-policy.html#children

[50] The "Children" section of the Privacy Policy also describes policies that relate to the Pokémon GO Mobile Trainer Rewards program; this text is not included here, as I do not reference it at all in this testimony.

[51] This Promotion was only available from Best Buy locations and only for a limited time five years ago (between November 15th, 2013 and January 4th, 2014); therefore, it is reasonable to conclude that there are few, if any, existing customers in California who are still on this plan today. (See: Sprint. N.D. "Unlimited, My Way Student Offer, Student Verification Form." Accessed: December 12, 2018. http://images.bestbuy.com/BestBuy_US/en_US/images/abn/2013/hom/pr/115213_student-validation-form.pdf)

[52] Exhibit D-11: Sprint Response to Public Advocates Office DR 4-5.

speculate regarding, any other circumstances in which a parent may give or elect to make a Sprint device "available" to an end user that may be under the age of 13." (emphasis added).[53] Therefore, while Sprint claims that it provides additional data collection and management controls to primary account holders who provide a device to a child under the age of 13, the only *means* for Sprint to determine whether a primary account holder is allowed to utilize the controls described in the privacy policy is through the "Unlimited, My Way Student Promotion," which Sprint no longer offers and likely has very few, if any, active customers in California.

This is further confirmed by Sprint's own internal documents. **[BEGIN SPRINT CONFIDENTIAL]** [redacted] **[END SPRINT CONFIDENTIAL]**. Therefore, the only account holders who can utilize the additional data collection and management controls that Sprint describes in its Privacy Policy are customers who provided mobile devices to their children as part of the "Unlimited, My Way Student Promotion." Again, this promotion was only available five years ago for approximately seven weeks and only from Best Buy locations.

Public Advocates Office asked Sprint how parents may request to review the personal information collected from a child's device. Sprint responded:

> All Sprint account holders must be at least 18 years of age, so Sprint's system does not differentiate granularly enough to recognize an end user that is under 18 years of age. Accordingly, its system does not differentiate between end users associated with an

[53] Exhibit D-11: Sprint Response to Public Advocates Office DR 4-5

[54] Exhibit D-12: Sprint Response to Public Advocates Office DR 4-5 CONFIDENTIAL Attachment "Cal PA DR 004 - DR 4-5(f) and (g) - Employee Process.pdf"

account by his or her individual characteristics – account information is associated with a single account holder and not with any individual end user(s).[55]

However, this statement is misleading; while it might be true that Sprint does not differentiate between end users of an account *based on their individual characteristics*, they are at least able to differentiate "Unlimited, My Way Student Promotion," users **[BEGIN SPRINT CONFIDENTIAL]** [redacted] **[END SPRINT CONFIDENTIAL]** Even more generally, the account preferences and controls available to customers through Sprint.com show that primary account holders can set a variety of different preferences for each device associated with their account.[56] These preferences include blocking apps, third-party charges, adult content, texts, pictures, video, and more. Therefore, while Sprint does not differentiate between end users based on their individual characteristics, they are nonetheless *capable* of setting different controls for each device under the same account.

Another way the privacy policy does not accurately or adequately describe the rights of parents is in the sentence describing parents' right to review and delete their children's information. Referencing this paragraph of the privacy policy, the Public Advocates Office asked Sprint to describe the types of instances in which parents "may be able to review or request deletion of the personal information collected from a child's device, or take steps to prevent further collection of such information." Sprint responded that "No specific circumstances or "instances" are required for an account holder or parent to complete this review or request or to take such steps."[57] Therefore, Sprint's own policy is incorrect where the policy states, "In *some* instances, a parent *may be able* to review…"; according to Sprint, parents *are* able, and in *any* circumstance, to review or request deletion of the information collected from their child's device.

B. T-Mobile Does not Allow Parents to Exercise their Right to Control the Information Generated by their Children, as Required by Federal Law

T-Mobile describes the terms that relate to the collection of information about children in their Privacy Policy, under the heading "What Types Of Information We Collect About You":

---

[55] Exhibit D-13: Sprint Response to Public Advocates Office DR 1-96 and 1-102.

[56] Exhibit D-14: Sprint Response to Public Advocates Office DR 4-5 CONFIDENTIAL Attachment "Cal PA DR 004 - DR 4-5(f)(i) and (j) - Screenshots (002).pdf".

[57] Exhibit D-11: Sprint Response to Public Advocates Office DR 4-5.

> "We do not knowingly solicit children to purchase our services or products. If, however, you authorize a child to use our services or products by providing them a device associated with your account, any information associated with such use will be treated as your information in accordance with this Statement. If you are the primary account holder, you will have the ability to set the marketing preferences for any other lines on your account, including those for any children to whom you provide a device. Our websites are not designed to attract children under the age of 13 and we do not intentionally or knowingly collect Personal Information on our websites from anyone under the age of 13. We encourage parents to be involved in the online activities (including wireless Internet browsing) of their children to ensure that no information is collected from a child without parental permission."

According to T-Mobile's Privacy Policy, the company does not provide any additional protection to devices that belong to children, beyond what is already provided to customers of any age. Their policy specifically states that they do not "knowingly solicit children" to purchase their services or products and that they do not design their website to attract children, and do not "intentionally or knowingly" collect Personal Information from children. It's clear that T-Mobile certainly understands that some customers provide devices to children under the age of 13; but by stating that they don't "intentionally" collect information from children, and any information they do collect is associated with the primary account holder, they are able to evade their responsibility to comply with COPPA.

The Public Advocates Office asked T-Mobile to "…indicate how primary account holders are able to set the marketing preferences for all phone lines associated with their account," as stated in the Privacy Policy paragraph quoted above.[58] T-Mobile responded by referencing another section of their Privacy Policy that says: "We may send you communications about services or products we, or our partners, sell. We want to provide you with meaningful choices regarding our marketing communications, and *you may choose to limit or opt-out of some marketing communications from us at any time*" (emphasis added). Therefore, primary account holders may "set the marketing preferences" for devices associated with their accounts only by "opting-out" of interest-based advertising.[59]

---

[58] Exhibit D-15: T-Mobile Response to Public Advocates Office DR 1-96 and 1-101.

[59] Sprint, on the other hand, requires customers to opt-in to their interest-based advertising program.

Interest-based advertising describes the practice of a company tailoring advertisements to a specific user based on information they have about that user. T-Mobile's Privacy Policy states that they tailor their interest-based advertising "based on [the customer's] use of our services and products as well as other information obtained by us and our ad providers." This kind of ad targeting is not appropriate for children. Although T-Mobile allows users to opt out of the program, it is unclear the extent to which T-Mobile customers are even aware of this program, let alone their ability to opt-out of it, for either themselves or a device they may provide to a child.

Furthermore, because the opt-out provision applies only to the interest-based advertising program, opting out still does not preclude T-Mobile from sharing customer data with third-parties. Under the heading "De-Identified Information," T-Mobile's Privacy Policy states: "We may provide information that does not identify you personally to third-parties for marketing, advertising or other purposes." Thus, although a primary account holder can limit *some* marketing, customers are not able to limit data collection and use more generally.

Lastly, T-Mobile's policy does not give *any* user the ability to review or delete the data that T-Mobile collects about them, regardless of their age.

C. Conclusions

Overall, neither T-Mobile's nor Sprint's policy provides adequate protection of children's information. T-Mobile automatically enrolls all customer devices in their interest-based advertising program. While they allow all customers to opt out of the program, customers may not opt out of data collection and use more generally. In addition, T-Mobile does not give any user of any age the ability to have T-Mobile delete the data and information the company has collected about them. As a result, children who utilize T-Mobile services may have their data and information tracked, used, or shared in a way that is inappropriate given their age.

Sprint clearly has the *ability* to give these necessary protections to customers who choose to provide a device to a child and their Privacy Policy seems to suggest they offer these protections to their customers. However, it is still unclear whether the necessary protections apply to any device or only to devices that are signed up for the "Unlimited, My Way Student Promotion". Similarly, while Sprint's policy seems to give primary account holders the ability to delete the data associated with a device that belongs to a user who is under the age of 13, this

right likely only applies to customers who are signed up for the "Unlimited, My Way Student Promotion".

It also seems that neither company currently complies with the rights that COPPA gives parents to control the data their children generate. T-Mobile's argument – that they have no means to determine the age of their users – is consistent with previous statements made by the industry association CTIA, which has claimed that wireless carriers specifically cannot themselves provide special data collection and management controls and preferences for devices belonging to children because "wireless carriers have no visibility into device users' ages. A person must be over the age of 18 to subscribe to wireless services, but carriers have no basis for ascertaining the age of the user of a device on their networks at any given time."[60] As this chapter demonstrates, this claim is likely false. Sprint's policy and company practices suggest that Sprint can and has found a way to determine whether a device belongs to a child. Therefore, the carriers' claim that they "have no basis" for ascertaining the age of their users is simply a reflection of the carriers' desire to evade federal regulations under COPPA, and is not a reflection of any *actual* limitations on their technical or organizational capacity to do so.

Carriers should not abdicate their responsibility to protect their customers, even if doing so means being subject to additional consumer protection regulation. While parents certainly have an important role to play in helping protect and control the data their children generate, their active oversight should not be the only means for protecting this sensitive class of customers. As stated in the same Columbia Law Review article cited in the introduction to this chapter:

> "Parents are likely not immune from techniques used by companies to shape consumer perceptions, and parents—like most consumers—may not always review or understand the implications of a company's terms and conditions and privacy policy. Parental consent to data monetization should not be used to justify data collection and monetization practices that are harmful to the long-term interests of children."[61]

[60] CTIA opening comments on P. 18-03-014 at p. 18.

[61] Elvy, Stacy-Ann. 2017. "Paying for Privacy and the Personal Data Economy." Columbia Law Review 117 (6): 92. Pg. 1455.

Protections like COPPA exist, in part, to protect children's privacy and, in turn, their future, regardless of whether their guardians are themselves actively involved in its monitoring and control.

Moreover, research suggests that children from low income families may be less protected than those from wealthier families.[62] One study found that only 35 percent of parents making $20,000 or more have helped their children set up privacy settings for a social media site; for parents making less than $20,000 annually, this figure drops to 18 percent.[63] The same study also showed that 60 percent of wealthy respondents, but only 36 percent of low-income respondents, used parental controls or other means to block, filter, or monitor their child's online activities. Therefore, it seems that many parents might not be taking an active role in managing their child's digital footprint, and children in low-income households might be at an even higher risk.

Although Sprint's policy seems to give parents additional options for helping children monitor and manage their digital footprint, the terms of Sprint's Privacy Policy that apply to children are nonetheless confusing. Even Sprint's own staff seem confused about what rights the paragraph actually gives to account holders. Either Sprint's internal policies must change in order to ensure account holders may access the rights they are afforded by the Privacy Policy, or else the internal policy and staff guidance need to be updated. The Commission should require T-Mobile and Sprint to conduct a customer satisfaction survey on their respective company's data privacy policies including customer notice and understanding of those privacy standards, customer ability and accessibility to opt-in/opt-out of carriers' data collection, and customer notification and recourse when data are compromised or breached.

---

[62] According to the KIDS COUNT Data Center cited above, 17 percent of people under the age of 18 (1.6 million people) live in families with income below the federal poverty line. The National Center for Children in Poverty estimates that approximately 4 million children in California live in low-income families, defined as families with income of about twice the federal poverty threshold. (See: http://www.nccp.org/profiles/CA_profile_6.html)

[63] Madden, Mary. 2017. "Privacy, Security, and Digital Inequality: How Technology Experiences and Resources Vary by Socioeconomic Status, Race, and Ethnicity." Data & Society Research Institute.

III. CONCLUSION

This testimony summarizes the potential impact of the proposed transaction on consumer privacy and data security. Although the results of this analysis suggest that both T-Mobile and Sprint engage in practices that put customer privacy and data security at risk, the overall risk to customer privacy and data security would likely increase for Sprint customers following a merger with T-Mobile. Furthermore, as discussed in the Public Advocates Testimony of Dr. Lee Selwyn impacts on competition, the merger should be denied. Should the Commission fail to deny approval of the Joint Applications, the Commission should develop mitigating conditions that are enforceable, measurable, able to be tracked and monitored on an on-going basis that address the following areas:

- New T-Mobile should create an inventory of all third-party suppliers and subcontractors who have or will have access to New T-Mobile customer data. New T-Mobile should use this inventory to conduct regular, periodic reviews of suppliers' and subcontractors' data security and risk management policies and programs. New T-Mobile should require third parties notify and receive approval from New T-Mobile when providing subcontractors access to customer data.
- New T-Mobile should make third party risk management is a company-wide priority. New T-Mobile should ensure the Board of Directors and other senior leadership receive periodic updates from staff about the status of the company's third-party risk management programs. New T-Mobile should require staff to report to the board and senior leadership whenever a data breach occurs.
- New T-Mobile should require third parties to notify New T-Mobile staff within 24 hours of a data breach or suspected breach, whether the breach originates with the third party or their subcontractor. Supplier contracts should clearly state how suppliers must notify New T-Mobile in the event of a data breach and should require suppliers provide periodic reports and updates describing the breach investigation and all corrective or remedial actions taken.
- New T-Mobile should allow customers to identify devices that belong to children and establish a program that would give primary account holders increased control over the data generated by devices that belong to children. This increased control should include the ability for the primary account holder to control what data are collected and to have New T-Mobile delete the data that are collected. In addition, New T-Mobile should not collect or store any information from these devices, beyond what is necessary to provide service. New T-Mobile should also not use the data, even if the data are de-identified, for any purpose other than providing service to that device.

New T-Mobile should automatically preclude children's devices from inclusion in any interest-based advertising program, even if other types of customers must "opt-out."

- New T-Mobile should employ an independent consultant to conduct a customer satisfaction survey on their respective company's data privacy policies including customer notice and understanding of those privacy standards, customer ability and accessibility to opt-in/opt-out of carriers' data collection, and customer notification and recourse when data are compromised or breached. The independent consultant should work with the Public Advocates Office and other consumer groups that are parties in this proceeding on the survey methodology and design, and should share the results of the survey with them and the Commission.

ATTACHMENTS

ATTACHMENT A

Statement of Qualifications and Experience

My name is Kristina Donnelly. My business address is 505 Van Ness Avenue, San Francisco, California, 94102. I am a Public Utility Regulatory Analyst I with the California Public Utilities Commission ("CPUC") in the Communications and Water Policy Branch of the Public Advocates Office. I received a Bachelor of Science Degree in Mathematics from American University in Washington, D.C. in 2005 and a Master of Science degree in Natural Resources and Environmental Management from the University of Michigan in Ann Arbor in 2008.

I joined ORA in March 2018, where I work to advance the organization's mission and advocate on behalf of public utility customers. In my time with the Public Advocates Office, I have performed extensive research and analysis on a wide array of communications issues to inform the Public Advocates Office's decision-making and policy positions. I have also authored and/or contributed analysis to numerous Public Advocates Office comments, reports and filings on communications issues related to customer privacy (P. 18-03-014), affordability of utility services (R. 18-07-006), and the California Advanced Services Fund (CASF) (R. 12-10-012). Prior to my time with the Public Advocates Office, I was a Research Associate with the Pacific Institute, a non-profit organization, where I conducted water and energy policy research and analysis.