

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



Public Advocates Office

California Public Utilities Commission

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

- PUBLIC -

San Francisco, California
January 7, 2019

A.18-07-011 AND A.18-07-012 THE PUBLIC ADVOCATES OFFICE TESTIMONY EXHIBIT INDEX

Exhibit #	Document Name	Public Information	Contains Confidential T-Mobile Information	Contains Confidential Sprint Information
D-1	T-Mobile Supplemental Response to Public Advocates Office DR 4-22	X		
D-2	T-Mobile Supplemental Response to Public Advocates Office DR 4-22 Attachment "TMUS-CPUC-PA-00005629.Public_Enterprise Third-Party Information.pdf"	X		
D-3	T-Mobile Response to Public Advocates Office DR 4-26	X		
D-4	T-Mobile Response to Public Advocates Office DR 4-26 CONFIDENTIAL Attachment "TMUS-CPUC-PA-13000073(Highly Confidential - Attorneys Eyes Only).PDF"		X	
D-5	T-Mobile Supplemental Response to Public Advocates Office DR 4-22 CONFIDENTIAL Attachment "TMUS-CPUC-PA-00005641.Confidential.pdf"		X	
D-6	Sprint Response to Public Advocates Office DR 4-4			X
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"			X
D-8	Sprint Response to Public Advocates Office DR 4-4CONFIDENTIAL Attachment "Cal PA DR 004 - DR 4-4(a) - Model privacy language.pdf"			X
D-9	T-Mobile Privacy Policy	X		
D-10	Sprint Privacy Policy	X		
D-11	Sprint Response to Public Advocates Office DR 4-5			X
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"			X
D-13	Sprint Response to Public Advocates Office DR 1-96 and 1-102	X		
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"			X
D-15	T-Mobile Response to Public Advocates Office DR 1-96 and 1-101	X		

Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

Exhibit D-1

**T-Mobile Supplemental Response to Public Advocates Office
DR 4-22**

**BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA**

In the Matter of the Joint Application of Sprint)	Application No. 18-07-011
Communications Company L.P. (U-5112-C))	
and T-Mobile USA, Inc., a Delaware)	
Corporation for Approval of Transfer of Control)	
of Sprint Communications Company L.P.)	
Pursuant to California Public Utilities Code)	
Section 854(a))	

In the Matter of the Joint Application of Sprint)	Application No. 18-07-012
Spectrum L.P. (U-3062-C), and Virgin Mobile)	
USA, L.P. (U-4327-C) and T-Mobile USA, Inc.,)	
a Delaware Corporation for Review of Wireless)	
Transfer Notification per Commission Decision)	
95-10-032)	

[PUBLIC VERSION]

**T-MOBILE USA'S SUPPLEMENTAL RESPONSE TO THE CALIFORNIA PUBLIC
ADVOCATES OFFICE'S DATA REQUEST 004**

Dave Conn
Michele Thomas
Susan Lipper
T-Mobile USA, Inc.
12920 SE 38th St.
Bellevue, WA 98006
Telephone: 425.378.4000
Facsimile: 425.378.4040
Email: dave.conn@t-mobile.com
michele.thomas@t-mobile.com
susan.lipper@t-mobile.com

Suzanne Toller
Davis, Wright, Tremaine LLP
505 Montgomery Street, Suite 800
San Francisco, CA 94111
Telephone: (415) 276-6536
Facsimile: (415) 276-6599
Email: suzannetoller@dwtd.com

Leon M. Bloomfield
Law Offices of Leon M. Bloomfield
1901 Harrison St., Suite 1400
Oakland, CA 94612
Telephone: 510.625.1164
Email: lmb@wblaw.net

Attorneys for T-Mobile USA, Inc.

Dated: December 21, 2018

[REDACTED]
[REDACTED]
[REDACTED] [EHC - AEO] However, as noted above, T-Mobile does provide consumers with information about third-party apps and services available for use with devices and our network services at: <https://www.tmobile.com/responsibility/privacy/resources/device-apps>.

Supplemental Response to DR 4-22 re TRS 610

Subject to and without waiving its objections, T-Mobile responds to Cal PA's December 6, 2018 email request for additional documentation regarding T-Mobile form TRS 610 which was produced as part of the initial response to DR 4-22. In particular, Cal PA requested the following documents cross-referenced in TRS 610:

1. Enterprise Third Party (Supplier) Risk Assessment (ESRA) screening form
2. T-Mobile's Supplier Risk Management (SRM) questionnaire

Consistent with T-Mobile's communications with Cal PA on December 14, 2018 and December 17, 2018, T-Mobile notes that the TRS 610 has recently been updated (as of the first week of December) and a copy of the updated document is produced with this Supplemental Response. Also included is a copy of T-Mobile's new Cyber Assessment Questionnaire for vendors and suppliers that went into production in early October and entirely replaced the SRM Questionnaire, which was retired in November. See Supplemental Response Folder, documents beginning with Bates No. TMUS-CPUC-PA-00005629. In addition, T-Mobile is providing a copy of the legacy SRM Questionnaire referenced above. See Supplemental Response Folder, documents beginning with Bates No. TMUS-CPUC-PA-00005642. The ESRA Screening Form mentioned in the version of TRS-610 previously produced refers to the SRM Questionnaire, which was both the intake screening form and the cyber questionnaire under the legacy program.

Supplemental Response to DR 4-22 re TISS 310

On December 5, 2018, Cal PA sent an email request for additional documents listed in Section 8 of TISS 310 that was other produced as in the initial response to DR 4-22. Those six documents are identified below:

1. TISD-1000 Information Handling Procedure
2. TLP-200 Records Management Policy
3. TLS-210 Records Retention Schedule Standard
4. TLP-500 Customer Location Information Policy
5. Non T-Mobile Worker (NTW) Classification list
6. THRP-102 Non T-Mobile Worker (NTW) Policy

Subject and without waiving its objections above, T-Mobile further objects to the email request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, the various internal policy and procedure documents have no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate

review of the Sprint Wireless Transfer Notification. T-Mobile also objects to this Data Request on the grounds that the documents requested are not responsive to the Data Request regarding preloaded apps; as explained to Cal PA, T-Mobile often cross references documents for ease of internal reference. The requested documents address the various unrelated matters described in their titles such as documentation retention policies.

Notwithstanding any of these objections, and as a courtesy to Cal PA, T-Mobile has provided a copy of the requested documents. See Supplemental Response Folder, documents beginning with Bates No. TMUS-CPUC-PA-00005601.

Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

Exhibit D-2

**T-Mobile Supplemental Response to Public Advocates Office
DR 4-22 Attachment “TMUS-CPUC-PA-
00005629.Public_Enterprise Third-Party Information.pdf”**

Enterprise Third-Party (Supplier) Information Security Standard

Approved by: Cyber Security & Privacy Policy Approver

1 HERE'S THE DEAL

The purpose of this TISS-610 Enterprise Third-Party (Supplier) Information Security Standard ("Standard") is to define T-Mobile's third-party information security requirements that help meet T-Mobile's overall risk management and security objectives.

Note – This Standard is aligned to the Enterprise Third-Party (Supplier) Risk Management Program. T-Mobile will complete an Enterprise (Supplier) Risk Management Program (ESRAP) intake for all Suppliers. The Cyber Assessment is triggered based off the results of the ESRAP intake.

2 WHAT'S IN-SCOPE

This Standard applies to all T-Mobile Third-Parties (suppliers) and T-Mobile personnel responsible for managing the supplier(s). This standard defines the security requirements that must be evaluated upon collaborating, changes in-scope-of-work and changes in the vendor security environment.

Third-Parties (Suppliers) includes, but not limited to, those performing any of the following:

1. Accessing, hosting, retaining, processing, or transmitting non-public T-Mobile information.
2. Developing, supporting, or managing technology, application(s), service(s), or solution(s) used for T-Mobile business purposes whether residing within T-Mobile's environment or hosted externally.
3. Any other work or partnership that, in T-Mobile's view, triggers a need to review or compare a party's processes, procedures, and policies.

3 ROLES & RESPONSIBILITIES

3.1 SUPPLIER

Supplier is responsible for completing cyber assessment questionnaire and adhering the security requirements in this Standard to implement appropriate technological, procedural, and physical requirements controls to protect T-Mobile customers.

3.2 T-MOBILE'S SUPPLIER CYBER RISK MANAGEMENT (SCRM) TEAM

SCRM partners with T-Mobile's Enterprise (Supplier) Risk Management Program (ESRAP) to ensure T-Mobile meets certain compliance and regulatory obligations to protect T-Mobile customers and information, as defined in the Scope. As part of T-Mobile's broader Digital Security Organization (DSO), SCRM performs detailed Cyber Assessments to ensure suppliers are compliant with the Standard.

4 T-MOBILE THIRD-PARTY (SUPPLIER) INFORMATION SECURITY REQUIREMENTS

4.1 INFORMATION HANDLING REQUIREMENTS

All T-Mobile information must be classified when created/received regardless of where it resides, the form it takes, or the technology used to handle it to enforce appropriate handling procedures as indicated in this Standard.

4.1.1 INFORMATION CLASSIFICATION

T-Mobile has defined an information classification scheme to properly identify all T-Mobile information. The information classification levels are used throughout this Standard. T-Mobile will determine the classification of the information you will be accessing, processing, and/or storing. Suppliers with multiple engagements at T-Mobile, must adhere to the requirements of the highest classification level they will be accessing, processing, and/or storing.

4.1.2 INFORMATION HANDLING FOR CUSTOMER FACING APPLICATIONS, SYSTEMS AND ACTIVITIES

1. Customer-facing applications, systems, and/or activities that utilize Customer Proprietary Network Information (CPNI) must meet CPNI compliance requirements as defined in T-Mobile's [CPNI](#) requirements including practices for authentication of customers, notice of account changes, and unauthorized access incident tracking.
2. All systems/applications must be able to collect, track, and honor user preferences with respect to data collection including, but not limited to:
 - a. Display a prominent notice and obtain affirmative consent of the user when collecting sensitive information about them;
 - b. Capability to obtain and track consent and include links to a detailed notice, or
 - c. Provide the option of opting out of data collection.
3. CPNI information must be stored within the boundaries of the United States.

4.1.3 DISPOSAL OF INFORMATION ASSETS

All non-public T-Mobile information must be returned to T-Mobile or destroyed as defined in the contractual agreement. When Suppliers are performing media sanitation they must provide T-Mobile a certificate of destruction upon request. Please reach out to SCRM@T-Mobile.com for the form.

When destruction is carried out by a disposal vendor, it is essential the information is protected continuously from the time at which the information asset is sent for destruction, until the time the disposal vendor has picked up the data.

The following destruction methods must be used where applicable (unless other methods are described in the contractual agreement):

Information Assets	Disposal Method
Paper	Cross-cut shredding, incinerating, or pulping such that there is reasonable assurance the materials cannot be reconstructed.
Mobile Computing Devices (cell phones, tablets, etc.)	Delete all non-public T-Mobile information on the device(s).
Electronic Storage Media (hard drives, USB/memory sticks, RAM, tapes, etc.)	Physically destroy or sanitize media in accordance to NIST-800-88 Guidelines for Media Sanitization and verify removal of data.
Optical Disks (CDs, DVDs, etc.)	Use optical disk shredder or disintegrator. Disks can also be incinerated or grinders can be used.

4.2 INCIDENT REPORTING

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.

4.3 ENCRYPTION REQUIREMENTS

Encryption technologies must be used to protect T-Mobile Confidential and/or Restricted information. T-Mobile Confidential and/or Restricted data must be encrypted at rest and in-transit (over public data networks and/or within the Supplier's internal network).

1. Information Transmission: SSHv2, TLS1.2 or higher.
2. Encryption Standard: AES, RSA
 - a. At Rest:
 - i. Symmetric: AES 256 or higher
 - ii. Asymmetric: RSAES-OAEP
 - b. In-Transit:
 - i. HTTPS, SSH, SFTP, Direct connection (dedicated circuit only for your scope of work with T-Mobile).
3. Usage of Proprietary Encryption Algorithm(s): must be reviewed, tested, and approved by T-Mobile.
4. Hashing Algorithm/Password Storage: SHA 2, Bcrypt, Scrypt, Other (upon approval of T-Mobile)
5. Wireless Networks: WPA2 (WPA1 and WEP must not be used)
6. MD5 and less must not be used

7. Unique T-Mobile encryption keys should be used for encryption of T-Mobile Confidential and/or Restricted information, where possible.
8. Salts must be random per user and a minimum of 16 characters in length.
9. User credentials must be encrypted during the authentication process when transmitted using a secure communications channel.
10. Passwords/authentication data must be hashed at rest any time the password is stored. Passwords must not be stored or transmitted in clear text (human readable form).

4.3.1 CRYPTOGRAPHIC REQUIREMENTS

Supplier must have clearly defined and documented processes for managing cryptographic keys.

1. Keys must be physically protected.
2. Keys must never be stored in locations that do not meet secure key management requirements.
3. Keys must be changed annually. Old keys must be retired or destroyed.
4. For high security keys, dual control or MFA must be implemented.
5. Key access must be restricted on a need to know basis.
6. Keys must be changed when employees with key access change job duties or leave the company.
7. Supplier using T-Mobile DNS domains must get their SSL/TLS certificates from T-Mobile.
8. All certificates used for T-Mobile purposes must have minimum key lengths of at least 2048 bits (RSA).
9. Passwords used to protect cryptographic keys must be as strong as the keys they protect.

4.4 ANTI-MALWARE

1. All systems supporting T-Mobile (e.g., external/internal servers, mobile computing systems, firewalls, web application firewalls, routers, and end User equipment) must be installed with current anti-malware software appropriate for their operating system, if applicable anti-malware technology exists.
2. Quick response procedures must be formally documented to detail actions in the event of a malware attack.
3. All anti-malware software must be actively running, updated with current definitions, and capable of generating logs. Centralized alerting must be enabled and monitored as part of the anti-malware solution.
4. End Users must not disable, bypass, or interfere with the anti-malware software security.

4.5 FACILITIES – PHYSICAL SECURITY

Physical security controls must be in-place to protect T-Mobile non-public information from unauthorized physical access, theft, and/or damage. The following controls are related to physical locations providing services to T-Mobile, including but not limited to: data centers, call centers, collection agencies, financial services, single tenant offices, multi-tenant offices, invoice processing, etc.

1. T-Mobile non-public information must be physically secured when not in use, including but not limited to, papers, manuals, and electronic media.
2. All areas of the premises storing and/or processing T-Mobile non-public information must be housed in secure areas and protected by a defined perimeter with appropriate security barriers and entry controls.
3. Facilities must be protected by intrusion alarms.
4. Alarms must be monitored twenty-four (24) hours per day, three hundred sixty-five (365) days per year.
5. Data centers must be equipped with dry fire suppression equipment or appropriate fire suppression equipment to prevent water damage to equipment supporting T-Mobile.
6. Access must be restricted to authorized personnel only.
7. Visitors must be required to present government issued photo identification prior to receiving access. Visitors awarded access to non-public areas must be escorted at all times in any area supporting T-Mobile.
8. Visitor logs must be maintained to provide an auditable trail of visitor activity. Visitor logs must be readily available for one year.
9. Visitor badges must expire automatically at the end of the work day.
10. Access rights to facilities must be based on business need and regularly reviewed and updated.
11. Access rights to facilities must be removed immediately upon notification of separation or a change in job responsibilities that no longer require physical access to the facility.
12. CCTV or other surveillance devices must be used to monitor individual physical access to sensitive areas and exterior entries where appropriate. The collected information must be reviewed and correlated with other entries. This data must be stored for a minimum of thirty (30) days for areas storing, processing, or transmitting T-Mobile non-public Information.
13. Physical access controls must exist for all network devices (e.g., wireless access points, gateways, and routers), data centers, telecommunications network facilities, and ancillary areas (e.g., generator, or UPS storage rooms); to ensure appropriate access by authorized individuals only.

4.6 CHANGE MANAGEMENT

Suppliers must have documented change management processes. Changes to all systems and applications supporting T-Mobile must be properly approved, developed, tested, and implemented in a controlled and consistent manner to provide a level of confidentiality, availability, and integrity consistent with the importance of the services provided.

1. Changes on all network devices, applications, systems or databases include:
 - a. Application changes – code or configuration
 - b. Application patches
 - c. System updates or patches
 - d. Hardware changes
 - e. Emergency changes
 - f. Production data changes
2. Documented change control process must exist to include:
 - a. Technical documentation and relevant user manuals must be updated.
 - b. Documented evidence of approvals and testing.
 - c. Testing plans and results must be documented and retained.
 - d. Back-out plans must be documented prior to implementation.
 - e. Emergency change procedures must be documented to include an established emergency approval authority.

4.7 NETWORK SECURITY

Appropriate network security controls must exist in Supplier's environment to ensure the confidentiality, integrity, and availability of the network, network devices, and information which support T-Mobile. If any of the following areas are not technologically possible, Supplier must notify SCRM@T-Mobile.com for determination of acceptable mitigation.

1. Appropriate network security controls must exist within Supplier's network to protect the network segment dealing with T-Mobile non-public information. The capability of Users to connect to and transmit/share T-Mobile non-public information between shared and segregated networks must be restricted on a least-privilege basis.
2. Network must have routing controls enabled to ensure access control requirements are met and the network is protected from breaches or attacks.
3. All access control lists and firewall rule sets related to systems supporting T-Mobile must be reviewed and approved by Supplier's management at least every 6 months.

4.8 DATA ACCESS MANAGEMENT

1. The Supplier is responsible and accountable for managing assets containing T-Mobile non-public information that are under the Supplier's control, and responsible for security controls relevant to any Supplier access to such assets.
2. Supplier with access to T-Mobile Confidential and/or Restricted information must have annual security and privacy awareness training programs based on the relevant role and responsibilities within the organization.

3. In a multi-tenant environment, there must be the ability to logically or physically segment data such that data may be accessed for a single tenant only, without inadvertently accessing another tenant's data (e.g., using unique identifiers or different schemas for each tenant).
4. If data will be stored, accessed, processed, and/or retained outside of the United States of America, the Supplier must contact ESRAP@T-Mobile.com for review and approval.
5. Back-up data containing non-public T-Mobile information must be segregated (physically or by using unique identifiers) from Supplier's information and Supplier's client's/customer's information with appropriate access controls to prevent unauthorized access.
6. If mobile devices will be utilized to transmit, receive, or store T-Mobile non-public information, a mobile device management solution must be used with the capability to remotely lock and wipe lost/stolen devices and to enforce disposal of information.

4.8.1 LOGICAL ACCESS CONTROLS

1. Access right to systems accessing, processing, and/or storing T-Mobile non-public information must be granted on a least privilege basis. Access rights must be reviewed at least every 90 days. Inactive User accounts with no activity for more than 90 days must be removed and/or disabled.
2. Remote access to T-Mobile's environment(s) must be approved by a management-level single point of contact of the Supplier that will be responsible for enforcing T-Mobile security requirements.
3. MFA must be implemented for all remote elevated (privileged) network access for systems supporting T-Mobile.
4. User IDs must be unique and assigned to specific individuals.
5. User access rights to systems or information supporting T-Mobile must be deactivated within 72 hours upon Supplier's employee/contractor voluntary termination or change in job duties no longer requiring access. In the event of an involuntary termination, access must be removed immediately.
6. Creation of local admin groups and/or file shares must be added based on minimum necessary permissions and role-based appropriateness.

4.8.2 PASSWORD COMPLEXITY

1. Passwords (including default passwords) must be changed upon installment of the system or application, prior to launch in a production environment.
2. Group, shared, or generic accounts and passwords must not be used. Accounts must have an identified owner.
3. Passwords must not be displayed in clear text when being entered.
4. Systems must maintain a record of previous passwords and prevent re-use of at least the last 5 previously-used passwords.
5. Systems must lock accounts (User, Admin/Privileged, Service) after 30 minutes of idle activity or after 5 consecutive invalid login attempts.

The following are requirements for Account Types supporting or accessing T-Mobile environments.

Account Type	Requirements
User	<ol style="list-style-type: none"> 1. Passwords <u>must</u> contain a minimum of 8 characters, and require: a mix of upper and lower case characters, include at least 1 number, and include at least one special character. 2. First time passwords <u>must</u> be a unique value and system <u>must</u> force password change on first use. <i>Note: If User chooses first password value, system does not need to force password change on first use.</i> 3. Password changes <u>must</u> be forced at least every 90 days.
Admin/ Privileged	<ol style="list-style-type: none"> 1. Passwords <u>must</u> contain a minimum of 15 characters or, if not technically feasible, the system maximum. Passwords <u>must</u> meet the same complexity requirements as User accounts. 2. Admin/Privileged accounts <u>must</u> be separate from User accounts. 3. Passwords <u>must</u> be changed for all systems and user administrative accounts user had access to when user leaves organization or changes roles. 4. Password changes <u>must</u> be forced at least every 90 days.
Service (aka system passwords)	<ol style="list-style-type: none"> 1. Passwords <u>must</u> contain a minimum of 30 characters (60 is preferred), and <u>must</u> meet same complexity requirements as User accounts. A password generation tool should be used to generate randomized passwords. 2. <u>Must not</u> be given interactive root or local administrator rights. 3. Passwords <u>must</u> be changed at least annually, or earlier in the case of security issues. 4. Passwords <u>must not</u> be shared beyond those with a demonstrated need to know. 5. Systems <u>must not</u> be able to select and change its own service account passwords. 6. Passwords <u>must</u> be immediately changed when a person with knowledge leaves the organization or changes roles. 7. Passwords <u>must not</u> be placed in ticket tracking systems.

	8. <u>Must</u> only be used for their approved service and not shared with systems/applications for which they were not provisioned.
--	--------------------------------------------------------------------------------------------------------------------------------------

4.8.3 SEGREGATION OF DUTIES

Segregation of duties (aka separation of duties) refers to dividing roles and responsibilities so that a single person cannot subvert a critical process.

1. Software developers must not have access to write/update/migrate code or changes to code in production systems.
2. Users must not be responsible for auditing the systems they are also responsible for maintaining.
3. While implementing segregation of duties, the principles of least privilege and need-to-know must be implemented.

4.9 SECURE SYSTEM AND SOFTWARE DEVELOPMENT

Note: This section applies to systems or applications specifically developed or customized for T-Mobile. It may not apply to commercial off-the-shelf software without any customization.

1. Software applications must be developed based on industry best practices and include security through the software development life cycle (SDLC). T-Mobile may request documentation on Supplier's SDLC process. SDLC must use the following minimum guidelines:
 - a. Defined duties based on job responsibility.
 - b. Separate development, test, and production environments.
 - c. Application code must be limited to appropriate personnel.
 - d. Test data, vendor default accounts, tests accounts and passwords must be removed before production systems become active or are released to customers.
 - e. Production data must not be used for development and testing.
 - f. Secure code review checklist followed to ensure the following elements are addressed: structure, documentation, inputs, invalid characters, variables, arithmetic operations, loops and branches, defensive programming, error handling, access control, authentication and session management, efficiency, and support.
2. Applications must have strong authentication mechanisms, including user of minimum passwords or PIN lengths, lockout enforcement after 5 consecutive invalid login attempts, and logging and monitoring of failed login attempts.
3. Custom code must be peer reviewed, documented, and tested for security vulnerabilities. T-Mobile may request the documentation related to such reviews and testing.
4. Applications with non-public T-Mobile information must be developed taking into consideration the sensitivity of the information being handled.

- a. Information must be masked during display in systems/applications where applicable (e.g., Social Security Numbers, bank account numbers, payment card information, passwords)
 - b. Cookies created for T-Mobile purposes may not be linked or linkable to an identifiable individual and must be encrypted and configured correctly. Sharing of cookies with third-parties must be as per the [T-Mobile Privacy Policy](#).
5. For customer facing applications, customer (or potential customers) must have the ability to create their authentication credentials, except for temporary credentials

4.10 VULNERABILITY & PATCH MANAGEMENT

Supplier must have documented, auditable vulnerability and patch management processes in-place for networks, hosts, and applications supporting T-Mobile. Processes must include, but are not limited to:

1. Vulnerability scans must be performed at least every ninety (90) days for the following:
 - a. Authenticated scans and un-authenticated scans must be performed for internal/external web applications, hosts, network and web applications.
 - b. Un-authenticated scans must be performed for external host and network scans.
2. Authenticated vulnerability scans must be performed for new systems/applications and/or enhancements to existing systems/applications prior to production deployment.
3. Supplier must retain vulnerability scan results supporting T-Mobile systems/applications for at least twelve (12) months from the date of the scan. Supplier must provide T-Mobile a copy of the most recent technical vulnerability assessment for systems supporting T-Mobile.
4. Supplier must ensure systems and applications are not operated past their End of Support lifecycle. All operating systems and applications must be on current, vendor supported versions (i.e., versions that still receive patches and updates) and Supplier must subscribe to vendor notifications of security threats and patches for each system/application supporting T-Mobile.
5. T-Mobile must be informed of vulnerabilities that may materially impact security as it relates to T-Mobile systems and data.
 - a. High vulnerabilities (e.g., CVSS Base score of 7.0 or higher) must be remediated within thirty (30) days of vendor release/notification.
 - b. Medium vulnerabilities (e.g., CVSS 6.9 to 4.0) - must be remediated within ninety (90) days of vendor release/notification.
 - c. Lower risk vulnerabilities (e.g., CVSS below 4.0) - must be remediated within one hundred eighty (180) days or as requested by T-Mobile.
6. Suppliers must develop, maintain, and test security baseline configurations (hardened configuration) for platforms/systems supporting T-Mobile based on industry-accepted standards (i.e., CIS/SANS, ISO, NIST).

4.11 AUDITING & LOGGING

All network and information systems used for T-Mobile, in conjunction with the terms of contractual agreements, must be auditable and include the following requirements:

1. T-Mobile Confidential and/or Restricted data must not be contained in log files.
2. Procedures must ensure system activities are monitored for authorized use, access, and logging.
3. Level of auditing & logging must take into consideration the criticality of the application/process/system, the value, sensitivity and criticality of the information involved, system interconnection, past audit results, misuse, and system infiltration.
4. Auditing and logging must cover events including, but not limited to: authorized access, privileged operations, service accounts, unauthorized access attempts, systems alerts or failures, initialization of the audit logs, changes to or attempts to change system security settings and controls, errors and faults.
5. All events in the logs must be time-stamped. System times (clocks) must be synchronized via NTP (Network Time Protocol) to ensure accuracy of logs.
6. Log file retention for systems, applications, and/or databases supporting T-Mobile information:
 - a. Must be stored to log server(s) or media that is difficult to alter;
 - b. Must be stored for a minimum of 6 months.

4.12 SERVICE PARTNER CALL CENTERS

This section applies to Suppliers performing Call Center activities on behalf of T-Mobile related to existing or prospective T-Mobile customers. For Call Center physical security requirements refer to [section 4.5](#).

1. The following is only allowed on production floors if pre-approved by T-Mobile in writing:
 - a. Paper and the ability to print T-Mobile information.
 - b. Usage of devices that may record audio, video and images. Any use of such equipment must comply with applicable law, and must be stored with security safeguards and access controls to limit access on a least-privilege basis.
 - c. Access to the Internet
 - d. Usage of Instant Messaging applications by agents with access to T-Mobile Confidential and/or Restricted information.
2. Computers supporting T-Mobile may only electronically connect to approved communication and support systems.
3. Call Centers handling T-Mobile's CPNI must have T-Mobile's annual security and privacy awareness training for workers with access to CPNI. Training sessions must be conducted, and materials distributed to personnel prior to commencement of services for T-Mobile. T-Mobile will determine if CPNI is in-scope.

4.13 EXTERNAL AUDITS

1. T-Mobile may request evidence of external audits and certifications.
2. Suppliers in scope for Sarbanes Oxley (SOX) and/or financial services must provide SSAE 16 or 18 SOC 1, Type 2 report upon request.
3. All suppliers in-scope for T-Mobile's PCI program must provide proof of PCI compliance, including but not limited to, their most recent (within the last 12 months) Attestation of Compliance for the scope of services supporting T-Mobile, for e.g., locations, payment applications, third-party service providers. T-Mobile reserves the right to request additional information/documentation, for e.g., Report on Compliance, Self-Assessment Questionnaire, compensating control worksheet, as needed. Supplier will document which PCI requirements they manage on behalf of or in coordination with T-Mobile.

5 QUESTIONS? - GET HELP

- Contact SCRM@T-Mobile.com with any questions.

6 EXCEPTIONS

All cases of non-adherence to a T-Mobile Information Security policy, standard or procedure must be reported to SCRM@T-Mobile.com for evaluation. All material Supplier risks associated with T-Mobile customers, systems, and data must be treated and disclosed to T-Mobile (SCRM@T-Mobile.com).

7 MORE INFO

1. [T-Mobile Privacy Policy](#)
2. [Supplier Code of Conduct](#)
3. [T-Mobile CPNI Information](#)

Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

Exhibit D-3

T-Mobile Response to Public Advocates Office DR 4-26

**BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA**

In the Matter of the Joint Application of Sprint)	Application No. 18-07-011
Communications Company L.P. (U-5112-C))	
and T-Mobile USA, Inc., a Delaware)	
Corporation for Approval of Transfer of Control)	
of Sprint Communications Company L.P.)	
Pursuant to California Public Utilities Code)	
Section 854(a))	

In the Matter of the Joint Application of Sprint)	Application No. 18-07-012
Spectrum L.P. (U-3062-C), and Virgin Mobile)	
USA, L.P. (U-4327-C) and T-Mobile USA, Inc.,)	
a Delaware Corporation for Review of Wireless)	
Transfer Notification per Commission Decision)	
95-10-032)	

**T-MOBILE USA’S RESPONSE TO THE CALIFORNIA PUBLIC ADVOCATES
OFFICE’S DATA REQUEST 004**

Dave Conn
Michele Thomas
Susan Lipper
T-Mobile USA, Inc.
12920 SE 38th St.
Bellevue, WA 98006
Telephone: 425.378.4000
Facsimile: 425.378.4040
Email: dave.conn@t-mobile.com
michele.thomas@t-mobile.com
susan.lipper@t-mobile.com

Suzanne Toller
Davis, Wright, Tremaine LLP
505 Montgomery Street, Suite 800
San Francisco, CA 94111
Telephone: (415) 276-6536
Facsimile: (415) 276-6599
Email: suzannetoller@dwt.com

Leon M. Bloomfield
Law Offices of Leon M. Bloomfield
1901 Harrison St., Suite 1400
Oakland, CA 94612
Telephone: 510.625.1164
Email: lmb@wblaw.net

Attorneys for T-Mobile USA, Inc.

Dated: December 3, 2018

Data Request 4-26.

T-Mobile's Privacy Policy states: "Where we allow third parties the capability of accessing data about your location that is derived from our network, we require those third parties to observe specific privacy and security protections consistent with this statement."

- *Please provide a copy of the third party contracts, agreements, or other documents that describe what specific data use, privacy, and security protections or practices you require when providing third parties access to customer data.*
- *Please describe how T-Mobile assesses, manages, and monitors risks posed by third party access to customer data.*

Response to Data Request 4-26.

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases "assess," "manages," "monitors," and "risks posed." T-Mobile further objects to this Data Request to the extent it is duplicative of DR 1-109. T-Mobile further objects to this Data Request on the grounds it seeks information which is neither germane to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile's specific requirements for third parties with the capability of accessing location data has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification. T-Mobile further objects to this Data Request on the grounds the disclosure of such information could constitute a breach of its supplier contracts.

Subject to and without waiving its objections, T-Mobile further responds that its current privacy policies, practices, and disclosures fully comply with our obligations under all applicable federal and state laws. T-Mobile further responds that it maintains a supplier data security and risk management standard, which is a policy applicable to suppliers handling T-Mobile Customer Information. See <https://www.t-mobile.com/our-story/working-together/suppliers/supplier-code-of-conduct> for that enterprise risk management standard, along with T-Mobile's supplier code of conduct.

T-Mobile further responds that it observes privacy standards and complies with applicable laws that require certain contractual safeguards for supplier processing of personal information (as defined in those applicable laws). It is T-Mobile's standard practice to use its contract forms and templates. Where suppliers require use of their own contract forms, T-Mobile compares the supplier's contract form to its own to ensure appropriate clauses and concepts are addressed sufficiently, including with respect to data security. For relationships with suppliers where the supplier will have access to T-Mobile's confidential information, including customer information, and that use T-Mobile's contract forms, T-Mobile uses a data security template that sets forth the supplier's obligations to maintain the security of that information. This template is typically included as "Exhibit B" to a master services agreement with that supplier. See Cal PA DR 004 Production Folder. The Exhibit B template is tailored to the individual needs of the supplier relationship during the context of negotiations. For example, for suppliers that provide cloud computing services or software development, T-Mobile may include additional data

security terms. Similarly, if a supplier does not process payments, certain terms governing the processing of payment card data may be omitted if they do not apply. The terms in the Exhibit B template work in tandem with the supplier security policy noted above.

Additionally, 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.

Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

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”**

Contains CONFIDENTIAL Information

Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

Exhibit D-5

**T-Mobile Supplemental Response to Public Advocates Office
DR 4-22 CONFIDENTIAL Attachment “TMUS-CPUC-PA-
00005641.Confidential.pdf”**

Contains CONFIDENTIAL Information

Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

Exhibit D-6

Sprint Response to Public Advocates Office DR 4-4

Contains CONFIDENTIAL Information

**BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA**

In the Matter of the Joint Application of Sprint)	
Communications Company L.P. (U-5112) and)	Application No. 18-07-011
T- Mobile USA, Inc., a Delaware Corporation,)	
For Approval of Transfer of Control of Sprint)	
Communications Company L.P. Pursuant to)	
California Public Utilities Code Section 854(a).)	
)	

In the Matter of the Joint Application of Sprint)	
Spectrum L.P. (U3062C), and Virgin Mobile)	Application No. 18-07-012
USA L.P. (U4327C) and T-Mobile USA, Inc.)	
for Review of Wireless Transfer Notification per)	
Commission Decision 95-10-032.)	
)	

**SPRINT SPECTRUM L.P.
RESPONSE TO THE CALIFORNIA PUBLIC ADVOCATES OFFICE'S DATA
REQUEST 004**

Stephen H. Kukta
Sprint Spectrum L.P.
900 7th Street NW, Suite 700
Washington, DC 20001
Telephone: 415.572.8358
Email: stephen.h.kukta@sprint.com

Earl Nicholas Selby
Law Offices of Earl Nicholas Selby
530 Lytton Avenue, 2nd Floor
Palo Alto, CA 94301
Telephone: 650.323.0990
Facsimile: 650.325.9041
Email: selbytelecom@gmail.com

Attorneys for Sprint Spectrum L.P.

Dated December 3, 2018

REDACTED – FOR PUBLIC INSPECTION

Data Request 4-4.

Sprint's Privacy Policy states:

"We may share personal information with third parties who perform services on our behalf."

- a. Please provide a copy of the third party contracts, agreements, or other documents that describe what specific data use, privacy, and security protections or practices you require when providing third parties access to customer data.
- b. Please describe how Sprint assesses, manages, and monitors risks posed by third party access to customer data.

Response to Data Request 4-4.

Sprint objects to this Data Request on the grounds that it is vague and ambiguous with respect to temporal scope and with respect to the phrases “third party/ies,” “agreements,” “other documents,” “data use, privacy, and security protections or practices,” “require” “access,” “customer data,” and “assesses, manages, and monitors risks.” Sprint further objects to this Data Request on the grounds it is overbroad and unduly burdensome. Sprint also objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireless Transfer Application nor reasonably calculated to lead to the discovery of relevant information. The data collected or otherwise used by Sprint has no bearing on any appropriate review of the Wireless Transfer Notification.

Subject to and without waiving its objections, as for item 4-4 a., please see the document provided at Bates range SPR-CAPAO-00006061 through SPR-CAPAO-00006064, which is a model sufficient to show Sprint's general privacy and data security requirements when sharing Sprint data, whether Confidential Information or Privacy Restricted Data, with a third party. In addition, please see the [BC] [REDACTED] [EC] which is discussed further below and provided at Bates range SPR-CAPAO-00006065 through SPR-CAPAO-00006070.

Sprint responds with regard to DR 4-4 b. that its [BC]

[EC]

Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

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”**

Contains CONFIDENTIAL Information

Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

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”**

Contains CONFIDENTIAL Information

Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

Exhibit D-9

T-Mobile Privacy Policy

Privacy Policy & Personal Information | T-Mobile

T-Mobile Privacy Statement

December 31, 2016

WHAT TYPES OF INFORMATION WE COLLECT ABOUT YOU

We collect information about you and your associated device(s) when you use our products or services or otherwise interact with us or with third-party services through our products and services. Examples of the types of information we collect include:

- **Personal Information**

"Personal Information" means information that we directly associate with a specific person or entity (for example, name; addresses; telephone numbers; email address; Social Security Number; call records; wireless device location). Personal information does not include "de-identified," "anonymous," or "aggregate" information – which are not associated with a specific person or entity.

- **Customer Proprietary Network Information (CPNI)**

Customer Proprietary Network Information, or "CPNI", is a subset of Personal Information that is generated in connection with the telecommunications services we provide to you. CPNI includes, for example, call details, call location information, and certain information about your rate plans and features. CPNI does not include your name, address, and phone number.

For more information see [CPNI](#)

- **Credit and Financial Information**

We collect information about your credit card or banking information, Social Security Number, and credit history for account opening, management and billing and collection purposes. Financial information we collect is governed by [T-Mobile's Financial Privacy Statement](#).

- **Network and Device Information**

We may collect information about your use of our network (or other carriers' networks when roaming domestically and internationally) and the device(s) associated with your account, network data related to WiFi usage and device, and performance information, as well as data relating to your use of our website, applications and other products and services.

- **Location Data**

We may collect your device's location whenever it is turned on (subject to coverage limitations).

- **Performance and Diagnostic Data**

We may collect performance and diagnostic data about your use of our network, networks you roam on, WiFi services or your device. For example, we may collect information about the performance of the device, signal strength, dropped calls, data failures, battery strength and other device or network performance issues. We may also collect information about applications on your device, the fact that an application has been added, when an application is

launched or fails to launch, and length of time an application has been running.

- **Telematics**

If you are a customer of the T-Mobile SyncUp connected car service, we, and our application provider, collect data from the SyncUp device in your car. This data includes driver behavior information such as acceleration and braking, speed, and RPM. The device also reports vehicle location via GPS and can report on common vehicle issues called Diagnostic Trouble Codes (DTC).

- **Video Data**

When you use a T-Mobile video application, for example T-Mobile TV, on your device, we may collect information about the programs you watch to determine customer viewing habits so that we can tailor video selections to you or our customers.

- **Back Up and Cloud Services**

Some devices may automatically upload to T-Mobile network servers information you have stored on the device and/or SIM card in order to facilitate specific functions. For instance, some devices may back-up your address book, photo album, or diagnostic data. You may choose to disable such uploads, but this may affect functionality of the device or your services. We may also provide you the ability to upload other information from your device to T-Mobile or third-party network servers. For instance, you may have the option to upload pictures, text messages, recordings, calendars, tasks, or notes.

- **Collection of Information About Children**

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.

HOW INFORMATION ABOUT YOU IS COLLECTED

T-Mobile collects information about you in three primary ways:

- **Information You Provide**

We collect information that you provide to us when you apply for, purchase, or use our products or services, or otherwise communicate with us.

For example, some of the ways you may provide information to us include:

- When you sign up for our voice or data services or purchase other products or services, we may collect personal contact, billing, and credit information.
- When you establish or modify an online account, we may collect user identification information, passwords, and/or security question responses that you will use for future sign-on.
- When you interact with our customer service representatives, enter information on our websites, submit survey responses, or pay for services, we may also collect Personal Information and other information. We may

monitor and record phone calls, e-mails, live chats, or other communications between you, your device, and our customer service representatives or other employees or representatives.

- When you use our services on a phone provided to you by an account holder.

- **Information We Collect Automatically**

We automatically collect a variety of information associated with your use of your device (on our network, when roaming, or in WiFi mode) and our products and services, some of which may be associated with you or another user on your account.

For example some of the ways we may automatically collect information include:

- Our systems capture details about the type and location of wireless device(s) you use, when the device is turned on, calls and text messages you send and receive (but we do not retain the content of those calls or messages after delivery), and other data services you use.
- We may also gather information about the performance of your device and our network. Some examples of the types of data collected include: the applications on the device, signal strength, dropped calls, data failures, and other device or network performance issues.

- **Cookies, Web Beacons, and Similar Technologies**

We may use, or we may engage third-parties to use on our behalf, cookies (small data text files placed on your computer or device) or similar technologies to identify your computer or device and record your preferences and other data so that our websites can personalize your visit(s), see which areas and features of our websites are popular, and improve our websites and your experience.

We may also use web beacons (small graphic images on a web page or an HTML e-mail) to monitor interaction with our websites or e-mails. Web beacons are generally invisible because they are very small (only 1-by-1 pixel) and the same color as the background of the web page or e-mail message.

The information we receive through cookies, web beacons and similar technologies may enable us to recognize users across devices, such as smartphones, computers, tablets or related browsers. Depending upon your device or computer, you may be able to set your browser(s) to reject cookies or delete cookies, but that may result in the loss of some functionality on our websites. If we combine or link cookie or web beacon information with Personal Information, we will treat the combined or linked information as Personal Information under this Statement.

- **Web Browsing Activity**

Our Websites. When accessing our websites, mobile websites and related applications and widgets designed for your device or web-based experience, we automatically collect certain information about your device and your visit, such as your IP address, browser type, date and time, the web page you visited before visiting our website, your activities and purchases on our websites, and other analytical information associated with the sites.

Other Websites. When your device's web browser utilizes our data services to access websites other than our own, we automatically capture information associated with your browsing activities, and measure and monitor network and Internet connection performance, throughput, latency, and similar network data.

Do Not Track Statement. Some browsers have incorporated "Do Not Track" features. Most of these features, when turned on, send a signal or preference to the websites you visit indicating that you do not wish to be tracked. Those sites (or the third party content on those sites) may continue to engage in activities you might view as tracking even though you have expressed this preference, depending on the sites' privacy practices. Because there is not yet a common understanding of how to interpret the DNT signal, we do not currently respond to the browser DNT signals when you use our services and products or interact with our websites or online services. We do allow you to exercise choice regarding the collection of information by third parties about your online activities over time and across third-party websites or online services for online interest based advertising purposes and to opt out of our interest-based advertising on your device, as described below.

- **Voice Controlled Applications**

If you use a voice-controlled application, that application may collect and record your requests and other information from you and your phone.

- **Retail Beacons**

We may use beacon devices in our retail locations that collect data about your device. These programs use signals from smart devices (like mobile phones and tablets) to track movement and wait times. Retail beacons collect a unique identifier that your device routinely transmits (e.g., a MAC address) and converts it to an identifier unique to T-Mobile. In some cases, we will use identifiers that are already routinely collected by the T-Mobile network in order to provide you with wireless service. We use aggregated data in order to understand general traffic trends in our stores. This helps us to better service our customers.

- **Information From Other Sources**

We may also obtain information about you from other sources. For example, we may receive credit information from third-party sources before initiating your service, or background information in connection with employment opportunities. We may also obtain updated address information from our shippers or other vendors. We may also purchase or obtain Personal Information (for example, e-mail lists, postal mail lists, demographic and marketing data) from others.

HOW WE USE INFORMATION WE COLLECT ABOUT YOU

We use the information we collect for a variety of business purposes, such as:

- To route your calls or message or otherwise provide you with service;
- To provide and bill for products and services you purchase and charge to your account;
- To deliver and confirm products and services you obtain from us;
- To verify your identity and maintain a record of your transactions and interactions with us;
- To provide customer and technical services to you;
- To create, modify, improve, enhance, remove or fix our network, products and services, and their performance;
- To identify and suggest products or services that might interest you;
- To make internal business decisions about current and future product and service offerings;
- To provide you customized user experiences, including personalized product

and service offerings;

- To protect our rights, interests, safety and property and that of our customers, service providers and other third parties; and
- To comply with law or as required for legal purposes.

Fraud Prevention

We may use Personal Information, including voice print recordings, account information (such as purchase patterns) and device information for investigations or prevention of fraud or network abuse. We provide fraud prevention services to banks or other third parties. As part of this service, we may verify your phone number to help those third parties prevent your personal information from being used for fraudulent purposes. We also may provide the information you report as spam to 7726 to a third party to prevent fraud or network abuse, and we may share such information with government agencies and others that work to combat spam and prevent fraudulent, deceptive, and unfair practices.

Information Collected from Cookies

We may also use information collected from cookies or other similar technologies to improve our websites, make recommendations, and complete transactions you request.

Marketing

We may use information we collect to contact you about T-Mobile or third-party products, services, and offers that we believe you may find of interest. We may contact you by telephone, postal mail, e-mail, or other methods. You may opt-out of receiving marketing communications from us at any time as outlined below in [Choices Regarding Use of Your Information](#).

Directories

We do not publish directories of our customers' wireless numbers; nor will we provide or make such numbers available to third-parties for listing in their public directories, without the customer's prior consent.

Performance, Diagnostics & Management

We collect information about devices, our network and WiFi usage to perform diagnostic analyses and understand how your device is performing overall. Diagnostic data helps us troubleshoot technical issues related to your device's performance such as battery life, dropped calls, processing speed, device memory, service coverage, and network and WiFi signal strength that you and other customers may experience. If you are using a device in WiFi mode, we may collect information about that usage, such as the routing address and IP address. We also may use diagnostic data to identify and recommend products and services.

Location-Based Services

We use location information to route wireless communications and to provide 911 service, which allows emergency services to locate your general location. We may disclose, without your consent, the approximate location of a wireless device to a governmental entity or law enforcement authority when we are served with lawful process or reasonably believe there is an emergency involving risk of death or serious physical harm.

Depending on your device, you may also be able to obtain a wide array of services based on the location of your device (for example, driving directions, enhanced 411 Directory Assistance, Find My Device, or search results, etc.). These data services, known as Location-Based Services ("LBS") are made available by us and others,

usually via applications. These services use various location technologies and acquire location data from various sources.

These applications and services use various location technologies (including Global Positioning Satellite ("GPS"), Assisted GPS ("AGPS"), cell ID and enhanced cell ID technologies) to identify the approximate location of a device, which is then used in conjunction with the application to enhance the user's experience (for example, to provide driving directions, to provide enhanced 411 Directory Assistance, or search results, etc.)

LBS may, or may not, involve any interaction with or dependency on our network, and location-based services may or may not look to our network to obtain location data. Where we allow third parties the capability of accessing data about your location that is derived from our network, we require those third parties to observe specific privacy and security protections consistent with this statement.

It is important that you understand the location capabilities and settings of your device, and that you carefully read and understand the terms under which these services are provided – whether by us or another entity.

You should carefully review the privacy statements and other terms of third-parties with whom you have authorized the sharing of your location information, and you should consider the risks involved in disclosing your location information to other people.

Where we provide a location-based service, you will receive notice of the location features of the service and collection of location data is with your consent. You will be provided options for managing when and how such information should be shared (except in the case of certain parental controls or similar services associated with enterprise or multi-line accounts – for example, T-Mobile's FamilyWhere™ services – which may be managed solely by the primary account holder or their designee, but always with notice to the end-user). T-Mobile follows the CTIA's Best Practices Guidelines for Location-Based Services, which are available [here](#).

For more information on location services, see [Location Services](#)

Telematics

Data from our SyncUp connected car service is used to provide you with that vehicle monitoring service, to enable the functions of the SyncUp associated Motion app, and to enable WiFi connectivity in your car. In addition, your data may be shared with our application provider in order to enable third-party services that use your personal data, though in such cases no third-party will be granted access to data that identifies you without first obtaining your consent. We may also use such data for any of the other purposes listed in this statement, such as internal analysis, or to personalize offers we provide to you.

Advertising

You may see advertisements when you visit our websites, mobile websites, in mobile applications, or on your device. We may help advertisers better reach our customers by providing certain information, including device type, geographic information, language preferences or demographic information obtained from other companies to allow advertisers to determine which ads may be more relevant to you. However, we do not share Personal Information for advertising purposes outside of our corporate family without your consent.

Some examples of the types of advertising you might see include:

Our Ads on Our Websites. We may provide advertisements, such as banner ads, on our websites, mobile websites, and in mobile applications and widgets you may download, access or use on your device.

Other Company Ads on Our Websites. You may also see third-party advertisements

on some T-Mobile websites, services, or in applications, or on devices. These third-party advertisers, or their ad networks, may place or access cookies, web beacons, or similar technologies on your device, or use your device identifier, and may collect certain anonymous or de-identified information about your visit on our websites. The third-party advertisers who provide these ads may use this information to provide you with advertising on our websites, as well as on other websites. We do not have control over or access to any information contained in the cookies that are set on your computer or device by ad servers, ad networks, or third-party advertisers.

Our Ads on Other Websites. We may ask third-parties to place advertisements about our products and services on other websites, mobile websites and in mobile applications and widgets. The use of cookies, web beacons, or similar technologies by such third-parties on other websites is subject to any applicable privacy statements that they may have, not this Statement.

Interest-Based Ads

You may receive ads from us and our ad providers that are tailored to your interests. These interest-based ads are selected based on your use of our services and products as well as other information obtained by us and our ad providers. None of this information is Personal Information.

- We do not provide your Personal Information to third-party advertisers without your consent.
- Advertising may be tailored to the interests that advertisers have inferred from your browsing of our websites or other websites or applications with which the third-party partners to provide advertising.
- We may provide third-party advertisers with aggregated or de-identified location, demographic or similar data (unrelated to your browsing activities) that does not personally identify you. This data may be used by advertisers to help tailor their ads on our websites, and on other sites and applications.
- We, and our providers, may use a de-identified profile of your web-browsing and application use activity and interests. This profile does not contain information that identifies you personally, but may include a unique or encrypted identifier that enables your device to be matched to a profile of your browsing activity and de-identified characteristics about your interests.
- When we use information associated with your web browsing activities on websites that are not our own to provide interest-based advertising or offers, we will provide you with notice and appropriate choice.

For more information see [T-Mobile Ad Options](#)

Choices About Advertising

T-Mobile adheres to the Digital Advertising Alliance's ("DAA") Self-Regulatory Principles for Online Behavioral Advertising.

- *On Your Mobile Device.* Where we offer interest-based ads, you can opt-out of certain interest-based advertising by clicking on the ad options link on or near the advertisement or by clicking [here](#).
 - If you turn off interest-based ads, you will still see just as many ads, but the ads may not be based on your interests and may be less relevant to you.
 - Your choice only affects the ads you see on websites and applications you access on your device.
 - If your device's browser cookies are deleted, or your device is reset, you may need to reset the interest-based ads feature.
 - If you are using your device, but are not on our network (such as a WiFi

network), we, and our ad providers, may not be able to identify your ad choices.

- *On Your Computer or Non-Mobile Device.* For information about targeted advertising, or to opt-out of use of your browser information for purposes of certain third-party advertising, please visit www.aboutads.info/choices. Please note that if you opt out, you will continue to receive the same number of ads, but they may be less relevant because they will not be based on your interests. You may still see ads related to content on a web page or based on other nonpersonal information. Please note that this opt-out is cookie-based. If you change computers or devices, change web browsers, or delete cookies, you will need to visit the aboutads site and opt-out again.

HOW WE STORE AND PROTECT THE INFORMATION COLLECTED ABOUT YOU

Protecting Your Information

We use a variety of physical, electronic, and procedural safeguards to protect Personal Information from unauthorized access, use, or disclosure while it is under our control.

We provide password protected online access to your account information through my.t-mobile.com. For multi-line accounts, the primary account holder is authorized to access online account information for all the devices and lines on the account. Other users may generally access online account information related only to their respective device and line (for example, if a parent provides a device to their child, the child may access online information about that device and line— including CPNI). The primary account holder, however, may designate additional or more limited access rights for other users on the account.

Under federal law, you have a right, and we have a duty, to protect the confidentiality of CPNI and we have adopted statements and procedures designed to ensure compliance with those rules. We will not intentionally disclose your CPNI to third-parties without your permission, except as allowed under FCC rules, applicable law, or explained in this Statement. However, if you are the primary account holder, you may designate other "authorized users" (for example, a spouse) to access and manage your account information, including CPNI. For more information see [CPNI](#)

Retention and Disposal

We retain information only for as long as we have a business or tax need or as applicable laws, regulations, or government orders require. When we dispose of Personal Information, we use reasonable procedures designed to erase or render it unreadable (for example, shredding documents and wiping electronic media).

HOW YOU CAN UPDATE YOUR INFORMATION AND CHOOSE HOW WE CONTACT YOU

You may access and modify your contact information by visiting my.t-mobile.com or a T-Mobile retail store, or by contacting Customer Service. You may also contact us using the information in the [How to Contact Us](#) section below.

Choices Regarding Use of Your Information

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. Although you may elect not to receive marketing information from us, if you subscribe to our services or buy our products, you will continue to receive invoices, customer-service and transactional notices, and similar communications. The Primary Account Holder can configure options for marketing communications for all lines on the account.

If you are a T-Mobile customer and you manage your account online, you can manage your preferences regarding marketing communications by logging into your my.t-mobile.com profile. If you do not manage your account online, or you are not a current T-Mobile customer, you may manage your preferences regarding marketing communications [here](#).

You may also manage your preferences regarding marketing communications by contacting Customer Service by dialing 611 from your T-Mobile phone or 1-844-349-4189 from any phone, or, with respect to marketing e-mails, by following the "unsubscribe" instructions on any marketing e-mail we send you.

See also [Marketing Choice](#)

Do Not Call Registry

The FTC maintains a National Do Not Call Registry at <https://www.donotcall.gov/>, and your state may maintain its own Do Not Call Registry. Putting your number on these Registries also may limit our telemarketing calls to that number.

YOUR ROLE IN PROTECTING YOUR PRIVACY

You play an important role in ensuring the security of Personal Information. We encourage you to use safeguards to protect your information and devices. For more information please see [Protecting Your Privacy](#).

OTHER INFORMATION YOU SHOULD KNOW

Consumer Code for Wireless Service

We follow the [Consumer Code for Wireless Service](#) established by the Cellular Telecommunications & Internet Association ("CTIA"). In doing so, we want to help customers understand their bills, receive quality service, and make informed choices and conform our information practices under this Statement to meet the requirements of applicable federal and state laws and regulations.

Your California Privacy Rights

California Civil Code Section 1798 entitles California customers to request information concerning whether a business has disclosed Personal Information to any third parties for the third parties' direct marketing purposes. As stated in this Statement, we will not sell or share your Personal Information with non-affiliated companies for their direct marketing purposes without your consent. California customers who wish to request further information about our compliance with this law or have questions or concerns about our privacy practices and statements may contact us as specified in the [How to Contact Us](#) section below.

PRIVACY STATEMENT UPDATES AND CONTACT INFORMATION

How We Communicate Changes to This Statement

We may update this Statement at any time to provide updates to or clarification of our practices. If we make changes, we will revise the date at the top of the Statement. If we propose to use Personal Information in a materially different way, we will provide you with notice by posting notice of the changes on our website for at least 30 days before we implement those changes, and obtain your consent as specified above for any material change regarding disclosure of Personal Information. You should refer to this Statement often for the latest information and the effective date of any changes.

How to Contact Us

If you have any questions or comments about this Statement or about T-Mobile's privacy practices, please call Customer Service at 611 (from a T-Mobile phone) or 1-844-349-4189 (from any phone) or send an e-mail message to privacy@t-mobile.com. You may also direct your privacy-related comments or questions to the address below:

T-Mobile USA, Inc.
Attn: Chief Privacy Officer
12920 SE 38th Street
Bellevue, Washington 98006

Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

Exhibit D-10

Sprint Privacy Policy

Español Business

Call to order 1-866-275-1411 Sign In ▾ Stores



My Sprint

Support

Shop

Activate

Search

[Legal / Regulatory and Consumer Resources](#)[Terms and Conditions](#)[Service / Product Specific Terms](#)[Sprint Forward Terms and Conditions](#)[Sprint Forward Important Service/Product Specific Terms](#)[Open Internet Information](#)[Privacy Policy](#)[Do-Not-Contact Policy](#)[Analytics and Behavioral Marketing](#)[CTIA Checklist](#)[CTIA Code of Conduct](#)[Account Management Tools and Usage Alerts](#)[Lost / Stolen Phones](#)[Legal Notifications](#)[Taxes and Surcharges](#)[Tariffs](#)[Consumer Resources](#)[Acceptable Use Policy](#)[Visitors Agreement](#)[Copyright Notice](#)[Social Contests and Promotions](#)[Unlocking Policy](#)

Sprint Corporation Privacy Policy

Last updated March 29, 2017

This Privacy Policy ("Policy") describes how Sprint Corporation ("Sprint") will collect, access, use or disclose your personal information. It applies to all of our products, services, and web sites ("Services"). A few of our Services are covered by different privacy policies and, in the event of a conflict between the two, the product, brand or service-specific policy governs. ([En Español](#))

Personal information does not include information that is not used to identify you, including aggregate or anonymous information. Our collection, access, use, disclosure and safeguarding of your personal information is subject to U.S. law.

[Information collected](#)
[Use of personal information](#)
[Information we share](#)
[Network and information security](#)
[Information choices and changes](#)
[Children](#)
[Contacting us](#)
[Updating this policy](#)
[Your California privacy rights](#)
[International data privacy policy](#)

INFORMATION COLLECTED

We collect personal information about you in various ways. We may also get information from other sources, including from affiliates, and may combine it with information we collect about you.

Information you give us. The personal information we collect includes information you give us, such as name, postal address, telephone number, e-mail address, date of birth, social security number or other government identification number, demographics, activities, location information, and personal preferences. You may give us information in a variety of ways, including when you sign up for Services, communicate with customer care or register on www.sprint.com.

Information that we automatically collect. We automatically receive certain types of information whenever you use our Services. We may collect information about your device such as the type, operating system details, signal strength, whether it is on and how it is functioning, as well as information about how you use the device and services available through it, such as your call and data usage and history, your location, web sites you have visited, applications purchased, applications downloaded or used, and other similar information. In addition, when you visit our website, we may collect information contained in HTTP headers such as IP addresses, information about your web browser, the pages you viewed and your history of navigating to a page.

We may link information we automatically collect with personal information, such as information you give us at registration or check out. We may use systems or tools to follow your use of our Services and other applications, including using cookies, web beacons and other mechanisms, along with analysis of network and device information. For example, we allow collection by analytic service provider(s) of site click-stream and cookie data to help track aggregate and individual use of our Services. We sometimes use cookies to enable features on our sites, such as the ability to save your shopping cart or set preferences. Advertisers and advertising networks that serve ads on our sites may also use their own mechanisms, including cookies. These third party cookies or tools are governed by the privacy policies of the entities placing the ads and are not subject to this Policy.

Español Business

Call to order 1-866-275-1411 Sign In ▾ Stores



My Sprint

Support

Shop

Activate

Search

[Secure Online Use](#)[Sprint Upgrade Policy](#)

Services. We use your personal information to do things like:

- Process your orders.
- Protect our rights and property and those of our customers.
- Respond to legal process and emergencies.
- Develop or inform you of new products and services.
- Anonymize or aggregate personal information for various purposes like market analysis or traffic flow analysis and reporting.
- Monitor, evaluate or improve our products, Services, systems, or networks.
- Customize or personalize your experience with our Services.
- Customize or [personalize online advertising](#) that provides you information about products and services of Sprint or others that may interest you, including co-branded offers.

[Back to top](#)**INFORMATION WE SHARE****DE-IDENTIFIED DATA**

We may share information that is de-identified or in an aggregated form that does not directly identify you.

For example, we share de-identified information as part of our participation in programs such as the Adobe Marketing Cloud Device Co-op and LiveRamp's Connectivity Services to better understand how you use our websites and apps across the various devices you use. This enables us to deliver tailored promotions and customize your experience when you visit our sites.

- Visit <https://cross-device-privacy.adobe.com> to learn more about the Adobe Marketing Cloud Device Co-op, including how to manage your choices relating to this linking of devices.
- Visit <https://liveramp.com/privacy/> to learn more about LiveRamp's Connectivity Services. You can also opt out of having your information collected as part of this program by visiting <http://www.aboutads.info/choices/>.

We also share de-identified or aggregate information for purposes such as to:

- Conduct market or traffic flow analysis and reporting or produce or facilitate production by others of business and marketing reports to share with third parties. For example, we may aggregate customer information across a particular region and create a report showing that 10,000 subscribers from a given city visited a sports stadium. If you do not wish for us to use your information to produce de-identified and aggregated data sets in the reports we share with third parties, you may opt out at any time. Click [here](#) for details.
- With your opt-in consent only, customize or personalize advertising based on information we collect about your use of your wireless device in order to provide wireless service to you. For example, we may use information about your mobile web browsing or use of mobile applications to deliver advertisements tailored to your interests, and we may share de-identified information about your use of your device with third parties so that they can tailor advertising to your interests based on that information. To participate in this program, you must opt in. Click [here](#) for details on how to do so.

[Back to top](#)**PERSONAL DATA**

We do not share information that identifies you personally with third parties other than as follows:

Affiliates. We may share personal and non-personal information with affiliated entities for approved business purposes. The data may include credit-related, payment history and transactional information. View Sprint's Financial Privacy Notice on [sprint.com/privacy](https://www.sprint.com/privacy) or by

Español Business

Call to order 1-866-275-1411 Sign In ▾ Stores



My Sprint

Support

Shop

Activate

Search



family customers and other group account holders ("Group Accounts"). The account holder for Group Accounts is the entity or person that buys the service or product for its employees, family members or other authorized users. You (as the user of a device) may receive service, certain pricing, terms or other benefits through a Group Account with us. If so, we may share with that Group Account holder customer registration and other information related to your use of our services.

Relationship, Discount, and Reward Programs. We may share limited personal information (e.g., name, address, telephone number, account status/active or inactive, membership number) with non-Sprint entities when you sign up for a discount or reward program, including when you sign up for a service discount through the Sprint Discount Program, for eligibility verification, fulfillment, and administrative purposes.

Third Party Verification Services. We may share limited personal information (e.g., address, phone number) with non-Sprint entities to assist with identity verification, and to prevent fraud and identity theft.

Other Third Parties with Your Consent. We may share information with other third parties with your consent. For example, you may agree to our sharing your information with other third parties to hear about their products and services. Use of the information you agree to share will be subject to those third parties' separate privacy policies. This may include sharing information collected in connection with financial products or services, such as installment billing. View Sprint's Financial Privacy Notice at sprint.com/privacy.

Disclosures to Third Party Application and Service Providers. You may choose to use services and products offered by third parties through our Services or devices, such as third party applications. When you leave our network you may also use mobile roaming services provided by third parties. Your use of such services and applications may result in these third parties collecting your personal information and obtaining information from Sprint, including location information (when applicable). You may also choose to give personal information directly to third parties when using our Services. In each case, personal information you give a third party will be subject to its terms, conditions, and policies—not this policy. You should review a third party's privacy policy and terms of service before providing your information or using the service.

Business Transfers. Personal information about you may be disclosed as part of any merger, acquisition, sale of company assets or transition of service to another provider. In the unlikely event of an insolvency, bankruptcy or receivership, personal information may also be transferred as a business asset.

Protection of Sprint and Others. We may access, monitor, use or disclose your personal information or communications to do things such as:

- comply with the law or respond to lawful requests or legal process;
- protect the rights or property of us, our agents, members, our customers, and others including to enforce our agreements, policies and terms of use;
- respond to emergencies;

[Back to top](#)

NETWORK AND INFORMATION SECURITY

We maintain a variety of physical, electronic, and procedural safeguards. These safeguards help protect your personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction. Be sure to use a strong password to access your information on Sprint.com and not one you use for other services. You can learn more about how you can protect your information by reviewing our [privacy FAQs](#).

[Back to top](#)

INFORMATION CHOICES AND CHANGES

Español Business

Call to order 1-866-275-1411 Sign In ▾ Stores



My Sprint

Support

Shop

Activate

Search



related communications.

- You may register a do-not-contact request by calling Sprint customer care or sending an email to officeofprivacy@sprint.com. View Sprint's Do Not Contact Practices [here](#).
- If you register a do-not-contact request, we still may contact you for non-promotional purposes, such as emails or wireless messages related to your accounts or our ongoing business relations.

Advertising. As described above, we work with advertisers and advertising networks that serve ads or collect information on our sites and that may use cookies, web beacons and other technologies to collect information about your use of our sites. This information may be used to, among other things, analyze and track data, determine the popularity of certain content, deliver advertising and content targeted to your interests on other websites and better understand your online activity. To find out more about targeted advertising and/or to "opt out" of automatic collection of information for this purpose, visit <http://www.aboutads.info/choices/>.

Cookies. If you disable cookies on your Internet browser, you also may stop some collection and use of data when you visit our web sites.

Account Information. If you would like to change certain Sprint account information, you may create an online account and manage your account online. For more information, visit www.sprint.com.

[Back to top](#)

CHILDREN

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. In such cases, 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.


Sprint allows children under 13 to participate in the Pokémon GO Mobile Trainer Rewards program with their parent or guardian's consent. When a visitor under 13 attempts to register for Sprint's Pokémon GO Mobile Trainer Rewards program, we will ask for a parent or guardian email address in order to provide program details and seek parental consent for the child to participate. Detailed information about the program can be found [here](#).

If you believe your child is participating in Sprint's Pokémon GO Mobile Trainer Rewards program without your consent, please feel free to contact us using the contact information below. A valid request to delete a child's personal information will be accommodated within a reasonable time.

[Back to top](#)

CONTACTING US

If you have any questions or complaints that concern this Policy, please call us at Sprint or email us at officeofprivacy@sprint.com. If you prefer, you also may write us at Office of Privacy -Legal Department, Sprint, P.O. Box 4600, Reston, Virginia 20195. To send us a legal notice relating to this Policy, send it to Our Legal Notices Address listed in, and by the method specified in, the [Acceptable Use Policy](#).

[Español](#) [Business](#)Call to order 1-866-275-1411 [Sign In](#)  [Stores](#)[My Sprint](#)[Support](#)[Shop](#)[Activate](#) 

changing the date it was last updated or as required by law.

[Back to top](#)

YOUR CALIFORNIA PRIVACY RIGHTS

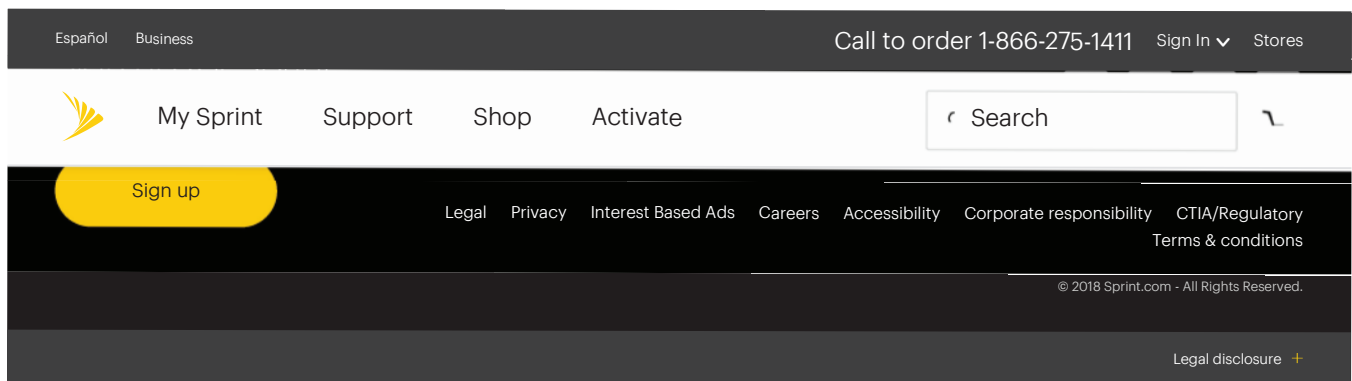
Sprint shares personal information between Sprint affiliates and marketing agents for marketing purposes. We do not share your personal information with unaffiliated third parties for their own independent marketing purposes without your consent. California residents may request the categories of personal information Sprint shared with third-parties for the third parties' direct marketing purposes during the previous calendar year, if any. To make your request, send an email to officeofprivacy@sprint.com. Written requests may be sent to the Office of Privacy -Legal Department, Sprint, P.O. Box 4600 Reston, VA 20195. Sprint will respond to these requests within 30 days. Requests that come to Sprint by other means may result in a delayed response.

[Back to top](#)

INTERNATIONAL DATA PRIVACY POLICY

Our [International Data Privacy Policy](#) informs you about our practices and policies regarding the collection, use, disclosure, transfer, storage, and processing of personal information collected outside the United States in connection with Services offered by Sprint, its subsidiaries, affiliates, and agents.

[Back to top](#)



Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

Exhibit D-11

Sprint Response to Public Advocates Office DR 4-5

Contains CONFIDENTIAL Information

**BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA**

In the Matter of the Joint Application of Sprint)	
Communications Company L.P. (U-5112) and)	Application No. 18-07-011
T- Mobile USA, Inc., a Delaware Corporation,)	
For Approval of Transfer of Control of Sprint)	
Communications Company L.P. Pursuant to)	
California Public Utilities Code Section 854(a).)	
)	

In the Matter of the Joint Application of Sprint)	
Spectrum L.P. (U3062C), and Virgin Mobile)	Application No. 18-07-012
USA L.P. (U4327C) and T-Mobile USA, Inc.)	
for Review of Wireless Transfer Notification per)	
Commission Decision 95-10-032.)	
)	

**SPRINT SPECTRUM L.P.
RESPONSE TO THE CALIFORNIA PUBLIC ADVOCATES OFFICE'S DATA
REQUEST 004**

Stephen H. Kukta
Sprint Spectrum L.P.
900 7th Street NW, Suite 700
Washington, DC 20001
Telephone: 415.572.8358
Email: stephen.h.kukta@sprint.com

Earl Nicholas Selby
Law Offices of Earl Nicholas Selby
530 Lytton Avenue, 2nd Floor
Palo Alto, CA 94301
Telephone: 650.323.0990
Facsimile: 650.325.9041
Email: selbytelecom@gmail.com

Attorneys for Sprint Spectrum L.P.

Dated December 3, 2018

REDACTED – FOR PUBLIC INSPECTION

Data Request 4-5.

In response to Data Request no.001 Questions 102 through 106 about the data collection, use, and control options for devices that are used by children, in addition to standard objections to language and relevance, Sprint stated:

Response: “Subject to and without waiving its objections, Sprint responds that 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 account by his or her individual characteristics – account information is associated with a single account holder and not with any individual end user(s). With regard to instances where an individual end user would potentially identify themselves to Sprint as being under 18 years of age, Sprint references its Response to DR 1-96.”¹

However, in Sprint’s Privacy Policy, under the heading “Children,” Sprint states the following:

“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](https://www.sprint.com/manage), and reviewing the My Preferences tab.”²

In light of the language Sprint uses in its Privacy Policy, please answer the following questions:

- a. Is the “Unlimited, My Way Student Promotion” available today? If so, please provide copies of or links to the marketing materials used to advertise this promotion.*
- b. In the paragraph above, do the conditions outlined between “Sprint takes steps...” through “...the My Preferences tab.” only apply to phones that are provided to children under the age of 13 as part of the “Unlimited, My Way Student Promotion”?*

¹ Response to Data Request no.001 Question 96: “Subject to and without waiving its objections, Sprint responds that it provides extensive information on its website in its Legal and Regulatory resources regarding its privacy policies, consumer options for protecting their data, and related topics, including but not limited to various way consumers can manage the use and sharing of their data. See e.g., <https://www.sprint.com/en/legal/legal-regulatory-and-consumer-resources>; see also <https://www.sprint.com/en/legal/sprint-corporation-privacy-policy.html>, and all Sprint privacy policies for individual apps that are available for purchase in various application stores (Google Play, iTunes, etc.).”

² <https://www.sprint.com/en/legal/sprint-corporation-privacy-policy.html#children>

- c. *Is the “Unlimited, My Way Student Promotion” the only option available for parents who want to provide a Sprint device to a child under the age of 13?*
 - i. *If not, what other options are available to parents who want to provide a Sprint device to a child under the age of 13? Please also identify which conditions, if any, from your privacy policy statement will apply when a parent provides a Sprint device to a child under the age of 13, through a method that is not through or associated with the “Unlimited, My Way Student Promotion.”*
- d. *Is the “Unlimited, My Way Student Promotion” available to children between the ages of 13 and 17 (inclusive)?*
 - i. *If not, what other options are available to parents who want to provide a Sprint device to a child between the ages of 13 and 17 (inclusive)? Please also identify which conditions, if any, in the paragraph above will apply when a parent provides a Sprint device to a child between the ages of 13 and 17 (inclusive), through a method that is not through or associated with the “Unlimited, My Way Student Promotion.”*
- e. *Please 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.”*
- f. *Please describe how parents are notified about their ability 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. Please include copies of any documents, employee training materials, or screenshots of relevant webpages, if applicable.*
- g. *Please describe how parents exercise the ability 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.*
- h. *Where you state, “Sprint takes steps to minimize the data it collects from Sprint applications on the device”:*
 - i. *Please describe the specific steps Sprint takes to minimize the data that it collects from Sprint applications.*
 - ii. *In Sprint’s response to Data Request no.001 Question 102, you state that your “system does not differentiate between end users associated with an account by his or her individual characteristics – account information is associated with a single account holder and not with any individual end user(s).” Please explain how Sprint minimizes the data that it collects from Sprint applications on devices that belong to children, in light of this statement.*
- i. *Please provide copies or screenshots of the resources you provide to parents to “control the information children can share with other parties.”*
- j. *Please provide us with screenshots of the “My Preferences” section of sprint.com/manage where parents may “control the content [their] children may access.”*

Response to Data Request 4-5.

Sprint objects to this Data Request on the grounds that it is vague and ambiguous with respect to temporal scope and with respect to virtually the entirety of this request. Among other deficiencies, the following phrases are vague and ambiguous: “marketing materials,” “advertise,” “conditions,” “option(s),” “available,” “provide(s),” “Sprint device,” “method,” “through or associated,” “types of instances,” “notified,” “ability,” “review or request,”

REDACTED – FOR PUBLIC INSPECTION

“personal information,” “collected,” “child’s device,” “take steps to prevent further collection of such information,” “exercise,” “deletion,” “steps,” “minimize,” “data that it collects from Sprint applications,” “devices that belong to children,” “copies,” “screenshots,” and “resources.” Sprint further objects to the request for “any documents, employee training materials, or screenshots of relevant webpages” as vague, ambiguous, overly broad, and unduly burdensome. Sprint also objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireless Transfer Application nor reasonably calculated to lead to the discovery of relevant information. For example, how customers use their devices and privacy settings has no bearing on any appropriate review of the Wireless Transfer Notification.

Subject to and without waiving its objections, Sprint indicates that its responses to *Data Request no.001 Questions 102 through 106* are fully consistent with its privacy policy. Sprint also specifically provides as follows:

- a. Sprint no longer offers the “Unlimited, My Way Student Promotion,” which was available only from mid-November 2013 to January 2014. Past marketing material is provided at Bates range SPR-CAPAO-00006071 through SPR-CAPAO-00006072.
- b. To the extent that Sprint currently has customers in California with active lines purchased under the “Unlimited, My Way Student Promotion,” Sprint responds that the conditions outlined by the Cal PA in DR 4-5 b. do not apply only to phones under the “Unlimited, My Way Student Promotion.”
- c. The “Unlimited, My Way Student Promotion” was the only promotion Sprint directed to parents of children under the age of 13, other than the Pokémon GO Mobile Trainer Rewards program, as enumerated in Sprint’s privacy policy. Sprint does not have knowledge of, and will not 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.
- d. The “Unlimited, May Way Student Promotion,” when it was available for purchase, was not available for an account holder to purchase for individuals between the ages of 13 through 17.
 - i. An account holder today may purchase a device for an individual between the ages of 13 and 17 in the same manner as the account holder would for any other individual over the age of 17, and no additional conditions would apply to such a purchase beyond Sprint’s standard terms and conditions. Sprint does not have knowledge of, and will not speculate regarding, any other circumstances in which a parent may “provide” a Sprint device to an end user who may be between the ages of 13 and 17.
- e. No specific circumstances or “instances” are required for an account holder or parent to complete this review or request or to take such steps.
- f. As indicated above, 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 speculate regarding, any other circumstances in which a parent may give or elect to make a Sprint device available to an end user who may be under the age of 13. With respect to the “Unlimited, My Way Student Promotion,” parents received privacy notification via the “Parental Notice” section of the Student

REDACTED – FOR PUBLIC INSPECTION

Verification Form at Bates number SPR-CAPAO-00006072, which references Sprint's privacy policy. In turn, Sprint's privacy policy outlines that process that parents may use to request that Sprint "delete any personal information provided to Sprint" (*i.e.*, calling Sprint Customer Care or contacting the Office of Privacy at Sprint's website). [BC] [REDACTED]
[EC] described at Bates number SPR-CAPAO-00006073.

- g. Please see the response to subsection (f) above, which outlines how parents exercise the ability to review or request deletion of the information in question. With respect to the "further collection of such information," please see Bates range SPR-CAPAO-00006072 through SPR-CAPAO-00006073.
- h.
 - i. Sprint conforms to industry standards and Federal requirements in minimizing data collected by applications.
 - ii. Sprint minimizes the data it collects from a device purchased under the "Unlimited, My Way Student Promotion" in accordance with the terms and conditions of the promotion and Sprint's privacy policy [BC] [REDACTED] [EC]
Sprint customers may utilize the MySprint app or their account portal to adjust their preferences regarding application data collection on any device.
- i. Please see documents provided at Bates range SPR-CAPAO-00006074 through SPR-CAPAO-00006087.
- j. Please see documents provided at Bates range SPR-CAPAO-00006074 through SPR-CAPAO-00006087.

Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

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”**

Contains CONFIDENTIAL Information

Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

Exhibit D-13

**Sprint Response to Public Advocates Office DR 1-96 and 1-
102**

**BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA**

In the Matter of the Joint Application of Sprint)	
Communications Company L.P. (U-5112) and)	Application No. 18-07-011
T-Mobile USA, Inc., a Delaware Corporation,)	
For Approval of Transfer of Control of Sprint)	
Communications Company L.P. Pursuant to)	
California Public Utilities Code Section 854(a).)	
)	

In the Matter of the Joint Application of Sprint)	
Spectrum L.P. (U3062C), and Virgin Mobile)	Application No. 18-07-012
USA, L.P. (U4327C) and T-Mobile USA, Inc.)	
for Review of Wireless Transfer Notification per)	
Commission Decision 95-10-032.)	
)	

**SPRINT SPECTRUM L.P. AND VIRGIN MOBILE USA, L.P.
RESPONSE TO THE CALIFORNIA PUBLIC ADVOCATES OFFICE'S
DATA REQUEST 001**

Stephen H. Kukta
Sprint Spectrum L.P. and Virgin Mobile USA, L.P.
900 7th Street NW, Suite 700
Washington, DC 20001
Telephone: 415.572.8358
Email: stephen.h.kukta@sprint.com

Earl Nicholas Selby
Law Offices of Earl Nicholas Selby
530 Lytton Avenue, 2nd Floor
Palo Alto, CA 94301
Telephone: 650.323.0990
Facsimile: 650.325.9041
Email: selbytelecom@gmail.com

Attorneys for Sprint Spectrum L.P. and
Virgin Mobile USA, L.P.

Dated October 10, 2018

HIGHLY CONFIDENTIAL INFORMATION – ATTORNEYS' EYES ONLY

Data Request 1-96.

In an Excel spreadsheet, please provide a list of the specific categories of data that You currently collect about individual consumers. For each type of data, indicate the following:

- a. A brief description of the data;*
- b. The name of the company that collects the data;*
- c. The original source of the data (e.g. provided by customer, collected automatically, collected from other sources, purchased from a third party, etc.);*
- d. How the data were collected (e.g. web browsing, microphone recording, text messages, phone calls, etc.);*
- e. The data format;*
- f. The frequency with which the data are collected;*
- g. The purpose or use of the data;*
- h. For each purpose or use of the data, indicate whether customers must opt-in or may opt-out;*
- i. The amount of time the data are retained;*
- j. Whether the data are shared with third parties. If yes, indicate:*
 - i. Under what circumstances the data are shared with third parties;*
 - ii. Whether the data are anonymized, aggregated, or otherwise de-identified before being shared with third parties;*
 - iii. Whether customers must opt in or may opt out of having this data shared;*
- k. Whether the data are sold to third parties. If yes, indicate:*
 - i. Under what circumstances the data are sold to third parties;*
 - ii. Whether the data are anonymized, aggregated, or otherwise de-identified before being sold to third parties; and,*
 - iii. Whether customers must opt in or may opt out of having this data sold.*

Response to Data Request 1-96.

Sprint objects to this Data Request on the grounds that it is vague and ambiguous with respect to the phrases “data” and “purpose or use of the data.” Sprint also objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireless Application nor reasonably calculated to lead to the discovery of relevant information. The type of data collected or otherwise used by Sprint has no bearing on any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, Sprint responds that it provides extensive information on its website in its Legal and Regulatory resources regarding its privacy policies, consumer options for protecting their data, and related topics, including but not limited to various ways consumers can manage the use and sharing of their data. *See e.g.,* <https://www.sprint.com/en/legal/legal-regulatory-and-consumer-resources>; *see also*

<https://www.sprint.com/en/legal/sprint-corporation-privacy-policy.html>, and all Sprint privacy policies for individual apps that are available for purchase in various application stores (Google Play, iTunes, etc.).

Data Request 1-102.

Indicate how parents may request to review the personal information collected from a child's device.

Response to Data Request 1-102.

Sprint objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases “personal information” and “collected from a child’s device.” Sprint also objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireless Application nor reasonably calculated to lead to the discovery of relevant information. The type of data collected or otherwise used by Sprint has no bearing on any appropriate review of the Sprint Wireless Transfer Notification. Sprint further objects to this Data Request on the grounds the information is equally available to the Cal PA.

Subject to and without waiving its objections, Sprint responds that 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 account by his or her individual characteristics – account information is associated with a single account holder and not with any individual end user(s). With regard to instances where an individual end user would potentially identify themselves to Sprint as being under 18 years of age, Sprint references its Response to DR 1-96.

Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

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”**

Contains CONFIDENTIAL Information

Docket: A.18-07-011 and A.18-07-012

Witness: Kristina Donnelly

Date: January 7, 2019

Public Advocates Office

Exhibit D-15

**T-Mobile Response to Public Advocates Office DR 1-96 and
1-101**

**BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA**

In the Matter of the Joint Application of Sprint)	Application No. 18-07-011
Communications Company L.P. (U-5112-C))	
and T-Mobile USA, Inc., a Delaware)	
Corporation for Approval of Transfer of Control)	
of Sprint Communications Company L.P.)	
Pursuant to California Public Utilities Code)	
Section 854(a))	

In the Matter of the Joint Application of Sprint)	Application No. 18-07-012
Spectrum L.P. (U-3062-C), and Virgin Mobile)	
USA, L.P. (U-4327-C) and T-Mobile USA, Inc.,)	
a Delaware Corporation for Review of Wireless)	
Transfer Notification per Commission Decision)	
95-10-032)	

**T-MOBILE USA’S RESPONSE TO THE CALIFORNIA PUBLIC ADVOCATES
OFFICE’S DATA REQUEST 001**

Dave Conn
Michele Thomas
Susan Lipper
T-Mobile USA, Inc.
12920 SE 38th St.
Bellevue, WA 98006
Telephone: 425.378.4000
Facsimile: 425.378.4040
Email: dave.conn@t-mobile.com
michele.thomas@t-mobile.com
susan.lipper@t-mobile.com

Suzanne Toller
Davis, Wright, Tremaine LLP
505 Montgomery Street, Suite 800
San Francisco, CA 94111
Telephone: (415) 276-6536
Facsimile: (415) 276-6599
Email: suzannetoller@dwt.com

Leon M. Bloomfield
Law Offices of Leon M. Bloomfield
1901 Harrison St., Suite 1400
Oakland, CA 94612
Telephone: 510.625.1164
Email: lmb@wblaw.net

Attorneys for T-Mobile USA, Inc.

Dated: October 10, 2018

Data Request 1-96.

In an Excel spreadsheet, please provide a list of the specific categories of data that You currently collect about individual consumers. For each type of data, indicate the following:

- a. A brief description of the data;*
- b. The name of the company that collects the data;*
- c. The original source of the data (e.g. provided by customer, collected automatically, collected from other sources, purchased from a third party, etc.);*
- d. How the data were collected (e.g. web browsing, microphone recording, text messages, phone calls, etc.);*
- e. The data format;*
- f. The frequency with which the data are collected;*
- g. The purpose or use of the data;*
- h. For each purpose or use of the data, indicate whether customers must opt-in or may opt-out;*
- i. The amount of time the data are retained;*
- j. Whether the data are shared with third parties. If yes, indicate:*
 - i. Under what circumstances the data are shared with third parties;*
 - ii. Whether the data are anonymized, aggregated, or otherwise de-identified before being shared with third parties;*
 - iii. Whether customers must opt in or may opt out of having this data shared;*
- k. Whether the data are sold to third parties. If yes, indicate:*
 - i. Under what circumstances the data are sold to third parties;*
 - ii. Whether the data are anonymized, aggregated, or otherwise de-identified before being sold to third parties; and,*
 - iii. Whether customers must opt in or may opt out of having this data sold.*

Response to Data Request 1-96.

T-Mobile objects to this Data Request on the ground that it is vague and ambiguous with respect to the phrases “data” and “purpose of the data.” T-Mobile also objects to this Data Request on the grounds it seeks information that is neither germane to the pending Wireline or Wireless Applications nor is reasonably calculated to lead to the discovery of relevant information; the type of data collected or otherwise used by T-Mobile has no bearing on any appropriate review of the Sprint Wireline Application or the Wireless Transfer Notification or T-Mobile’s compliance with the CPUC’s rules. T-Mobile further objects to this Data Request on the ground it is unduly burdensome as T-Mobile’s systems are not currently designed to provide the information at the level of detail requested.

Subject to and without waiving its objections, T-Mobile responds that its current privacy policies, practices, and disclosures fully comply with our obligations under all applicable federal and state laws. Further, T-Mobile provides extensive information on its website in the form of a Privacy Center regarding its privacy policies, consumer options for protecting their data and related topics including but not limited to various way consumers can manage the use and sharing of their data. See <https://www.t-mobile.com/responsibility/privacy>; see also <https://www.t-mobile.com/website/privacypolicy.aspx>.

Data Request 1-101.

For the individual CSA form provided in response to Questions 1-82 to 1-88, indicate how primary account holders are able to set the marketing preferences for all phone lines associated with their account.

Response to Data Request 1-101.

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrase “marketing preferences.” T-Mobile also objects to this Data Request on the grounds it seeks information which is neither germane to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information; the type of data collected or otherwise used by T-Mobile has no bearing on any appropriate review of the Sprint Wireless Transfer Notification or T-Mobile’s compliance with the CPUC’s rules. T-Mobile further objects to this Data Request on the grounds the information is equally available to the Cal PA.

Subject to and without waiving its objections, T-Mobile responds that, as a general matter, the account holder has the ability to manage the settings on the account. Further, T-Mobile provides extensive information on its website in the form of a Privacy Center regarding its privacy policies, consumer options for protecting their data, and other related topics including but not limited to the various ways consumers can manage the use of their data, advertising and marketing preferences. See <https://www.t-mobile.com/website/privacypolicy.aspx> (see section “Choices Regarding Use of Your Information”); see also <https://www.t-mobile.com/responsibility/privacy>; T-Mobile’s Response to DR 1-96.