Application: A.18-11-015
Exhibit No.: SDG&E-
Witness: Christopher Vera

UPDATED PREPARED DIRECT TESTIMONY OF

CHRISTOPHER VERA

CHAPTER 4

ON BEHALF OF SAN DIEGO GAS & ELECTRIC COMPANY

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

NOVEMBER 13, 2020

TABLE OF CONTENTS

UPDATED PREPARED DIRECT TESTIMONY OF CHRISTOPHER VERA - CHAPTER 4

I. INTRODUCTION

The purpose of this prepared direct testimony is to provide an update and supersede my testimony filed on November 26, 2018.[1] My testimony describes San Diego Gas & Electric Company's ("SDG&E") privacy concerns regarding Solution 1b (also referred to in this application as the "Alternate Solution"), including SDG&E's responsibility to safeguard customer privacy, the privacy risks and implications of Solution 1b, and SDG&E's recommendations for preserving customer privacy while making it as convenient as possible for customers to provide their consent to enable third parties to efficiently receive their utility data. While this testimony focuses on privacy risks related to Solution 1b, it must be noted that these same risks apply equally if not more so to Solution 1a.[2]

II. SDG&E'S RESPONSIBILITY TO SAFEGUARD CUSTOMER PRIVACY

In 2011, recognizing that energy usage data would fast become an asset collected by utilities and highly coveted by a myriad of third parties seeking access to this information for financial benefit, the State of California and the California Public Utilities Commission ("Commission" or "CPUC") established a robust collection of privacy rules that Investor-Owned Utilities ("IOUs") are required to follow. The Commission's Decision ("D.") 11-07-056, Adopting Rules to Protect the Privacy and Security of the Electric Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas

[1] This update testimony has been authorized by the Assigned Commissioner's First Amended Scoping Memo and Ruling (October 23, 2020) at 6.

[2] The Updated Prepared Direct Testimony of Tom Moses (Chapter 3) ("Moses Testimony (Chapter 3)") discusses the differences between Solution 1a and Solution 1b and the information technology and security considerations and concerns associated with those two proposals.

& Electric Company,[3] informally referred to as the "Smart Grid Privacy Decision," "adopts rules to protect the privacy and security of customer data generated by Smart Meters" and "policies to govern access to customer usage data by customers and by authorized third parties."[4] The Smart Grid Privacy Decision was later expanded to cover gas usage data, and data collected by gas utilities and Community Choice Aggregators ("CCAs").[5]

These rules further align with and support Public Utilities Code ("PUC") section ("§") 8380, which directs California energy corporations not to "share, disclose, or otherwise make accessible to any third party a customer's electrical or gas consumption data, except as provided in subdivision (e) or upon the consent of the customer."[6] PUC section 8380 further requires energy corporations to "use reasonable security procedures and practices to protect a customer's … consumption data from unauthorized access, destruction, use, modification, or disclosure."[7]

In June 2018, the State of California passed the Consumer Privacy Act of 2018 ("CCPA"), which went into effect January 1, 2020.[8] This new law introduced sweeping privacy requirements for companies that collect, sell or share consumer data, which included SDG&E customers. The law affords consumers "the right to request that a business that collects a consumer's personal information disclose to that consumer" the information the company has collected;[9] the purpose for which the personal information was collected; the categories of third parties with whom the business has disclosed consumer personal information to, and, subject to

---

3 *See* D.11-07-056.

4 *Id.*, at 2.

5 *See* D.12-08-045.

6 PUC § 8380(b)(1).

7 *Id.*, at § 8380(d).

8 Assembly Bill ("AB") 375, Stats. 2017-2018, Ch. 55 (Cal. 2018) and Senate Bill ("SB") 1121, Stats. 2017-2018, Ch. 735 (Cal. 2018).

9 *Id.*, at § 1798.100(a).

exceptions, to "request that a business delete any personal information about the consumer which the business has collected from the consumer."[10] Further, the law subjects companies who fail to "maintain reasonable security procedures and practices," to potentially significant financial penalties.[11] In accordance with the law, the California Attorney General drafted a set of regulations that became effective July 01, 2020 after final review by the Office of Administrative Law.[12] These regulations clarify several aspects of the CCPA and provide businesses direction in complying with the law. Finally, Proposition 24, the California Privacy Rights Act of 2020 ("CPRA"),[13] passed in November 2020. This law, whose company-applicable requirements become effective on January 01, 2023, overlays the CCPA and adds several new protections for consumer privacy, including broadening the definition of sensitive personal information, adding the right for consumers to make corrections to personal information collected about them, the right to opt out or limit the sale and sharing of their personal information, and significantly, mandates that businesses implement "reasonable security" over consumer personal information.

These privacy mandates have a direct effect on business decisions made by SDG&E when it comes to preserving customer privacy and sharing customer information with third parties. While SDG&E recognizes the value in making it easier to obtain customer consent, compliance with existing privacy law and regulations must be a principle concern when contemplating solutions for the click-through authorization process ("CTP").

The goal of the CTP is to make it easy and secure for customers to provide—and when necessary, to revoke— their consent to share data, usually in regard to participation in a third-

---

[10] *Id.*, at § 1798.105(a).

[11] *Id.*, at § 1798.150(a)(1).

[12] *See* State of California Department of Justice, CCPA, available at https://oag.ca.gov/privacy/ccpa.

[13] *See* CPRA, available at https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf

party program of their choice, while preserving their privacy. For the technical and security-related reasons described in the Moses Testimony (Chapter 3),[14] SDG&E concludes that the Alternate Solution does not meet the industry standards and requirements contained in State law and the Commission's Smart Grid Privacy Decision and may result in the unintended consequence of abuse by bad actors who seek to obtain and misuse customer information for their own purposes.

III. EXAMPLES OF MISUSE OF UTILITY SYSTEMS AND CUSTOMER INFORMATION IN DEMAND RESPONSE

Concerns for the potential of third-party abuse or misuse of utility customer information is not unfounded. Even where customer privacy protections exist, third parties have obtained and used confidential customer data to meet their own objectives rather than the customer's intended use. A few examples include:

A. Known third-party violations

In March 2017, SDG&E reported evidence of "screen scraping" practices to the CPUC in which at least one demand response provider ("DRP") collected My Account[15] usernames and passwords from SDG&E customers in violation of SDG&E's My Account terms and conditions for purposes of automatically logging into these customers' My Account to obtain their contact information, energy usage and related account data using automated software (*i.e.*, "screen scraping"). Beginning in June 2016, at least one other IOU also reported similar activity to the CPUC by a third-party DRP whose actions adversely impacted that utility's systems.

[14] *See* Moses Testimony (Chapter 3), Section VIII. Cost Estimate for Alternate Solution (OP 29, Bullet #2).

[15] My Account is described in the Prepared Direct Testimony of Neil Umali (Chapter 2), Section V. Whitepaper Response: Requests for Additional Data – Not Recommended.

B. Industry observations of misuse

As early as 2018, Nest, a manufacturer of smart thermostats, warned its customers of similar third-party "screen scraping" behavior on their website, which stated: "Companies that are not certified Works With Nest partners may ask you to use your account information to sign into their service. Other websites or apps may try to simply steal your account email and password by posing as a Works With Nest partner. Sharing your account email and password with unauthorized websites or apps can compromise the security of your home and personal information."[16] Google, parent company of Nest, has since updated this language to apply more broadly to a variety of security risks:

> Companies that do not have certified Works with Hey Google (or legacy Works with Nest) integrations, such as Starling, may also ask you to use your Google account information to sign into their service. When you enable an integration with a company that is not part of the Works with Hey Google program, the safeguards we would otherwise have in place cannot be used and there is a risk of exposing sensitive data to inadequate data protection, privacy, and security standards. You may even expose yourself and others to additional safety risks by using functionality in ways it wasn't intended. There may also be additional consequences to unapproved integrations, based on violations of Google's Terms of Service, such as a limitation in support or warranty coverage for Google products.[17]

C. Non-utility observations of misuse

The 2015-2018 Facebook data breach[18] involving third-party Cambria Analytics clearly demonstrated the risks posed by choosing convenient third-party access to customer data over reasonable standards-based security and privacy controls. Facebook provided access to sensitive customer data to a third-party researcher who in turn used this information for its own purposes.

---

[16] Nest, *Nest Support, Don't Share Your Account Email and Password, available at* https://nest.com/support/article/sharing-your-nest-account-email-and-password-with-other-companies-advertising-compatibility-with-nest, as of October 2018.

[17] *Id.*

[18] CNBC, *Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal* (April 10, 2018), *available at* https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html, as of October 2018.

This led to an inquiry by the Federal Trade Commission, Congressional hearings, and massive backlash from Facebook users. The effects of this breach are still being felt today, particularly in the State of California, and this significant event was one of several that led to the CCPA legislation.

IV. INDUSTRY STANDARDS SUPPORT SDG&E VALUES: CUSTOMER PRIVACY, CHOICE, INFORMED CONSENT

To counter both inadvertent and intentional threats to customer privacy, SDG&E advocates for industry-standard practices and technologies that are proven to have withstood the test of time and testing by security professionals to ensure these practices are working effectively. This is preferred over solutions that may appear convenient at the moment but too often result in the unauthorized use or acquisition of customer information, loss of customer trust, and possible violation of California law and Commission privacy regulations.

SDG&E subscribes to the use of standards-based best practices when it comes to securing customer data. The Open Authorization standard ("OAuth"),[19] described in the Moses Testimony (Chapter 3), and similar industry Internet standards, are open (meaning accessible and reproducible for use by companies like SDG&E) and widely used to reasonably ensure that the customer and no other has made an informed decision to consent to sharing their personal information during the CTP. Further, when using OAuth protocols, the customer cannot repudiate whether this action has occurred. If consent was given, all parties can be reasonably confident the customer indisputably provided it. This protects the third-party, the utility, as well as the customer.

[19] Internet Engineering Task Force, *The OAuth 2.0 Authorization Framework, RFC 6749* (October 2012), *available at* https://datatracker.ietf.org/doc/rfc6749/

V. THE ALTERNATE SOLUTION'S PRIVACY RISKS AND IMPLICATIONS

A. Brief description of the Alternate Solution

A detailed description of the technical aspects and technical security risks posed by the Alternate Solution can be found in the Moses Testimony (Chapter 3).[20] The Alternate Solution is a non-standard solution that requires critical customer authentication and authorization functions to move or pass through a non-trusted third party's infrastructure rather than remain within the trusted boundary of the utility. In a layperson's terms, this is roughly equivalent to a customer disclosing their debit card PIN number to a cashier, so the cashier can complete a sale. Previous intervenor comments and protests have argued this analogy is inaccurate. However, step 9 of the third party-proposed Solution 1 in Attachment 1 clearly indicates 2-factor tokens, parameters and codes being passed to the third party before the third party passes them to the utility.[21] This testimony will discuss the privacy implications of these security compromises.

B. The Alternate Solution Poses Privacy Risks

There are several privacy risks related to the Alternate Solution, which are described below.

Inability to reasonably identify the customer. The Alternate Solution requires the third-party to collect and share the necessary contact information about the customer to properly authenticate them. This contact information generally includes information that many people besides the customer may know (such as email address and phone numbers) and excludes information that is generally known only to the customer (such as their My Account credentials, account number, or portion of their social security number, which is common on many secure

[20] *See* Moses Testimony (Chapter 3), Section VIII. Cost Estimate for Alternate Solution (OP 29, Bullet #2).

[21] *See* Application 14-06-002, cons., Status Report Ordered by the Assigned Commissioner's Office During Discussions at the October 5, 2016 Click-Through Workshop (October 12, 2016), Attachment 1. *See also, e.g.,* Moses Testimony (Chapter 3) at TM-22-24.

websites involving the transacting of sensitive customer information). It is impossible for the utility to positively determine whether the information being provided is directly from the customer rather than the third-party or a malicious "man in the middle" who has compromised the transaction. This represents significant risk in positively identifying and authenticating the customer. Solution 1b's inclusion of a "two-factor" authentication (*i.e.*, requiring a code be generated and sent to the customer's email address or phone number) slightly reduces this risk but does not reasonably minimize it because the transaction requires accurate contact information previously provided by the customer to the utility to reliably complete the process. Outdated contact information could result in two-factor challenges not being delivered to the customer, or worse, to a party not involved at all in the transaction. Therefore, the Alternate Solution's privacy risk begins with a lack of reasonable trust that the utility on the downstream end of the process is interacting with the actual customer of record.

Lack of trust in proposed authorization. This privacy concern has to do with authorization, or the confirmation of what data the customer specifically intends to grant the utility permission to share with the third-party. In addition to collecting the customer's data as stated above, the Alternate Solution dictates that the third-party will also take responsibility for obtaining the customer's authorization (including details about what customer data the customer consents to share, such as meters, accounts, timeframes of authorization, etc.), which are critical components of the consent contract. If we assume momentarily that we had positively identified and authenticated the customer, despite the significant obstacles described above, the utility still would have no way to determine whether the customer's actual intent was being accurately conveyed to it by the third-party. Aggressive third parties, malicious actors acting as a "man in the middle," and even innocent third parties who have misconfigured their systems, could misrepresent what data the customer intended to share with the third-party. Under the Alternate

Solution proposed, the utility would have no choice but to rely on the third party's submission of the authorization as accurate and truthful without any reasonable validation by the customer.

Repudiation of customer consent. Because of the issues created by the Alternate Solution's authentication and authorization mechanisms, another problem is introduced: The absence of non-repudiation. Although both the third-party and SDG&E can log that a transaction took place, given the weakness in the aforementioned security controls, it is reasonably possible for a customer to deny that they were the party who authorized the specific consent transaction and neither the third-party nor the utility would have any reasonable means to disprove such an accusation. This would likely result in SDG&E being blamed for sharing a customer's energy usage (or other) data without proper authorization, potentially resulting in a reportable security incident per D.11-07-056.

Lack of security auditing controls. While the Commission can order utilities to implement specific security controls, such as auditing and logging, the third parties wishing to utilize the Alternate Solution answer to no comparable regulatory body. This means the inclusion of critical auditing controls in the Alternate Solution to determine what took place during the transaction should errors or illicit activity occur is dependent entirely on the third party's whim to include such controls, and such controls could be removed or disabled at any time if they are implemented at all. Further, it is unclear whether third parties will use uniform standards in customer privacy and information security controls or be transparent regarding their existing safeguards. While some third parties may do well at protecting customer information and auditing transactions, others may not adhere to even fundamental security requirements. Unfortunately, because there are no audit requirements or accountability measures for privacy and security by participating third parties, there is no way to tell the difference until after a security incident has occurred and even then, there is no mandate or incentive for poor-performing third parties to conform to any set of privacy, security or auditing standards. This

lack of formal accountability and auditing validation inflates the risks introduced by the Alternate Solution, and potentially and inappropriately transfers this increased risk to ratepayers, whose utilities do have such obligations. This contrasts with the current CTP in which the utility manages necessary security logging.

Difficulty with customer revocation of consent. Even assuming all other risks have been mitigated, a path for customer revocation remains unclear. While Resolution E-4868, dated August 24, 2017("Resolution") contemplates customer consent that "begins and ends on a third-party website,"[22] there is no such direction for revocation, which is a fundamental customer right. Customer revocation should be as easy to invoke as it was to provide consent in the first place. Solution 1b does not provide the customer any clear process to revoke their consent once granted and may confuse participating customers who have not directly interacted with the utility during the 1b process as to what they must do to revoke their consent should they so choose. Compare this to the existing CTP in which customers grant and revoke consent in the same place.

New legal risks. With enactment of the CCPA (and now the more recently enacted CPRA), California companies that meet specific criteria, including the IOUs, must apply stringent new privacy standards regarding customer reporting and, subject to exceptions, data deletion beginning in January 2020. The impact of these new privacy requirements on utility data sharing transactions remains unclear. While the effects of this new law are not unique to the Alternate Solution, the lack of non-standard authentication, authorization, accountability, and non-repudiation controls introduced by the Alternate Solution could run afoul of the utilities' need to maintain reasonable security practices. SDG&E expresses its concern that the Alternate

[22] Resolution at 5.

Solution may not be considered a "reasonable" security practice according to industry standards or the new law.

C. Consequences

The privacy risks discussed above result in the following consequences:

There will be a lack of utility standards-based trust. Utilities will have little confidence in whether the actual customer of record has authenticated into the process, and authorized their consent, or whether someone else impersonated them using information they know about the customer. Nor will the utility or the customer be able to trust that the authorization ostensibly received from the third-party is the customer's stated intent as there is no way to validate the scope of what the customer authorized against what the third-party conveyed to the utility.

Consequently, some risks may be inappropriately transferred to utilities. Because of the repudiation risks, customers will question the utility—not the third-party—when they believe they did not consent to sharing their information with a third-party. The utility will have been left with no ability to refute such claims.

There is also a lack of adequate security auditing. Neither the utility nor the Commission will have any record of what happened in the event a transaction error occurs, or the process is targeted by illicit behavior. Neither will the utility have the ability to hold third parties accountable to industry-standard privacy and security practices if their security auditing controls prove inadequate or non-existent. This consequence will make it difficult for the Commission to investigate complaints against third parties by customers, as allowed under Rule 32.

Customers will have no clear path to revoke consent. In addition to existing Commission privacy requirements, potential new legal liabilities require IOUs to evaluate their data sharing processes for reasonable security practices in order to minimize risk. The CCPA and CPRA introduce new privacy requirements that adversely impact utilities that use non-standard security practices to share sensitive customer data with third parties.

VI. CONCLUSION

As demonstrated by my prepared direct testimony, the legal and privacy concerns raised by the Alternate Solution cannot be adequately mitigated. To avoid these concerns, SDG&E recommends the Commission reject the Alternate Solution and instead continue with the current CTP.

This concludes my prepared direct testimony.

VII. STATEMENT OF QUALIFICATIONS

My name is Christopher Vera. I am employed by SDG&E as its manager of Office of Customer Privacy ("OCP"). My current responsibilities include overseeing SDG&E's customer privacy program, including compliance with California privacy law and Commission regulations affecting customer privacy. I assumed my current position in 2012. I have been employed by SDG&E since 2002 in its Information Security department and have held positions of increasing authority until assuming the role of OCP Manager. I am/was the lead author of the Cyber Security and Privacy section of SDG&E's 2012 Smart Grid Deployment Plan.

I have over 20 years' experience in the information and cyber security industry, including the development and management of several programs for the defense and energy sectors, including: incident response and e-forensics, vulnerability management, and security awareness and training, as well as the development of strategies, architectures, policies, standards and procedures for privacy and security compliance and governance programs. I am a Certified Information Systems Security Practitioner ("CISSP") and a member of the International Association of Privacy Professionals ("IAPP").

I have not previously testified before the Commission.

LIST OF ACRONYMS

AB	Assembly Bill
CCAs	Community Choice Aggregators
CCPA	California Consumer Privacy Act
CISSP	Certified Information Systems Security Practitioner
CPUC	California Public Utility Commission
CTP	Click-Through Authorization Processes
D.	Decision
DRP	Demand Response Provider
IAPP	International Association of Privacy Professionals
IOU	Investor-Owned Utilities
PUC	Public Utilities Code
SB	Senate Bill
SDG&E	San Diego Gas & Electric Company