

Data Privacy in the Digital Age: *What Consumers Really Think*

January 20, 2016



Agenda

- The Evolving Data Privacy Landscape
- Types of Consumers with regard to Privacy
 - Data Pragmatists
 - Data Fundamentalists
 - Data Unconcerned
- The Decline of the Data Fundamentalist
- Concerns Over Privacy in Gradual Decline
- Rising Public Awareness and Acceptance of Data Exchange
- The Rise of the Consumer Capitalist
- Incentives to Exchange Personal Information
- The Importance of Trust & Responsible Stewardship
- Current Real-World Examples of the Benefits of Sharing
 - Google Maps
 - Spotify “Discover Weekly”



Future Foundation/DMA/Axiom Consumer Surveys

- Data Privacy: What the Consumer Really Thinks is a survey-based report that has been conducted and published first in 2012 and again in 2015 in the U.K.
- The Future Foundation is a leading international consumer futures business
 - Core expertise based on identifying and forecasting social and consumer trends
- The DMA is a U.K.-based organization comprised of over 1,000 members
- Acxiom is an enterprise data analytics and SaaS company



The Evolving Data Privacy Landscape

- The digital revolution has challenged historic and contemporary views of privacy in our society
 - The true impact of the digital and data revolution on the notion of privacy is still very much in transition
 - Close to $\frac{3}{4}$ of respondents to the 2015 DMA/Axiom survey agreed that their definition of privacy is changing due to the internet and social media
 - This attitudinal evolution cuts across age groups
- Consumers are more aware of data and open to it being used as a part of everyday life
- Overall, the trend emerging is one of a more *aware, accepting* and *mature* consumer landscape
- It is crucial that policy makers keep up to date with fast-changing attitudes to privacy, and recognize that attitudes are neither uniform nor static

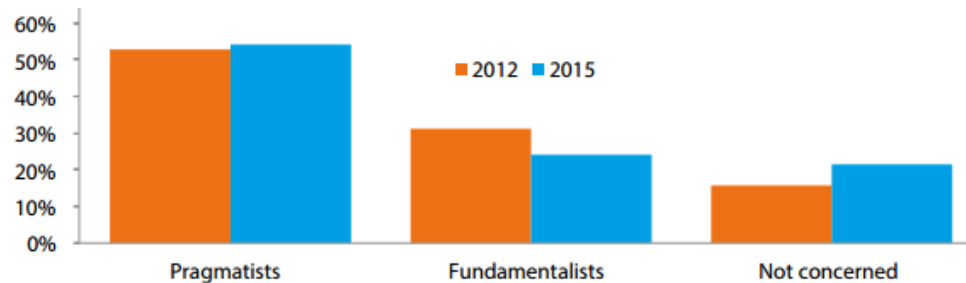
Types of Consumers with regard to Privacy

DMA/Axiom group consumers into three categories with regard to their attitudes toward privacy

- **Data Pragmatists:** those who will make trade-offs on a case-by-case basis as to whether the service or enhancement of service offered is worth the disclosure of the information requested
- **Data Fundamentalists:** those who are unwilling to provide personal information even in return for service enhancements
- **Data Unconcerned:** those who are unconcerned about the collection and use of personal information about them

The Decline of the Data Fundamentalist

- From 2012 to 2015, there has been a notable decline in consumers who identify as Data Fundamentalists
- There is a steady migration of attitudes toward a position of general acceptance
- Data Unconcerned are the fastest growing segment

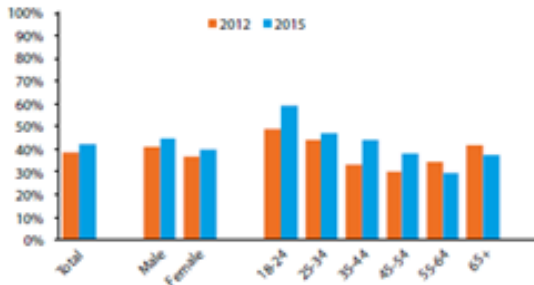


- Consumers' primary grievance is not sharing data *per se*, but rather not wanting to share data without a tangible benefit

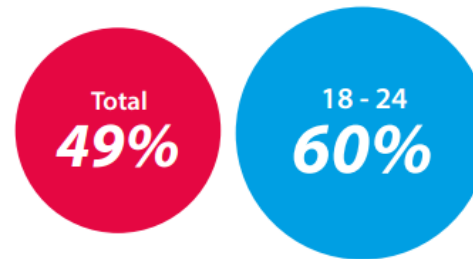
Concerns Over Privacy in Gradual Decline

- Overall, privacy concerns are declining as awareness of how and why data are collected grows

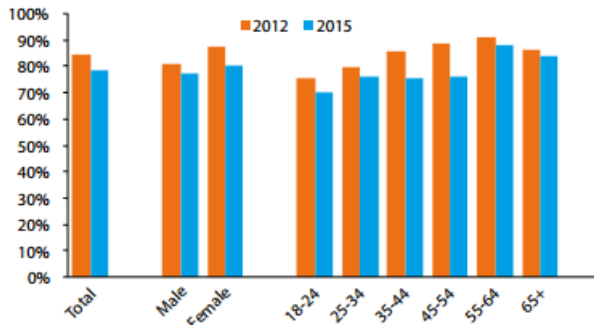
"As long as data doesn't get abused, privacy is less of an issue these days" | % who strongly agree or agree



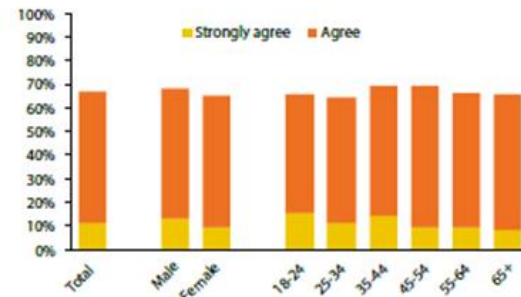
"I feel more comfortable with the idea of exchanging some personal data with companies than I did previously" | % who strongly agree or agree



"On a scale from 1 to 10 where 1 is 'not at all concerned' and 10 is 'very concerned'; how do you rate your levels of concern about the issue of online privacy these days?" | % who answer 7-10



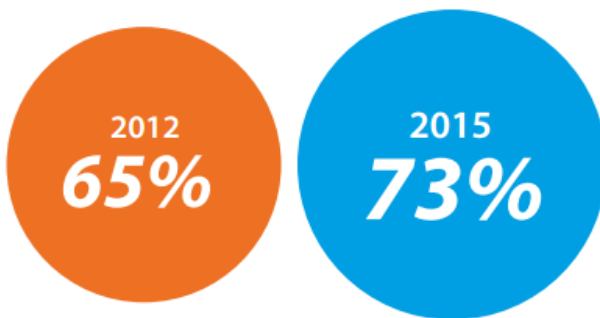
"I feel more aware of how my data is used and collected than in the past" | % who strongly agree or agree



Rising Public Awareness and Acceptance of Data Exchange

- Percentage agreeing that the exchange of personal data is essential for the smooth running of a modern society has leapt from 38% to 47%
 - Much of this growth is driven by 35-54s who are growing more comfortable with the value of modern data exchange than in the past
- Raw Data is of little usable value to consumers
 - Marketers can make use of this data for powerful insights and benefits
 - Consumers are far more likely to exchange data when a marketer can turn it into some form of useful insight or tool

"In the Internet age you expect to have to provide personal information in order to buy things" | % who strongly agree or agree



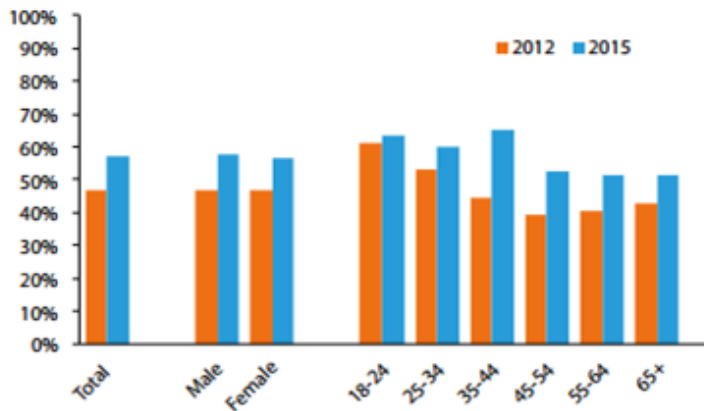
"Sharing data and personal information online is part of the modern economy" | % who strongly agree or agree



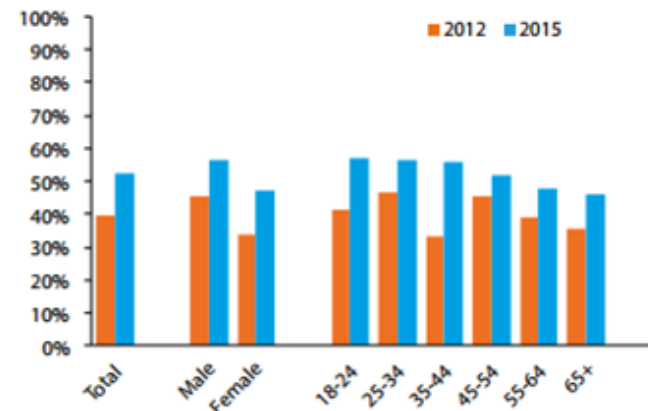
The Rise of the Consumer Capitalist

- Consumers are ever more aware of the value of their data, are asserting ownership of it and accepting the responsibilities that ownership implies
- Citizens increasingly see their personal data not as a manifestation of their privacy, vulnerable to the intrusion of snooping brands, but as a commodity “to be collected and traded to the benefit of the individual consumer”
 - The number of people who see their personal information as a way to command better deals from companies has increased from 40% to 52%

“I am happy to provide personal information in exchange for better services and offers” | % who strongly agree or agree

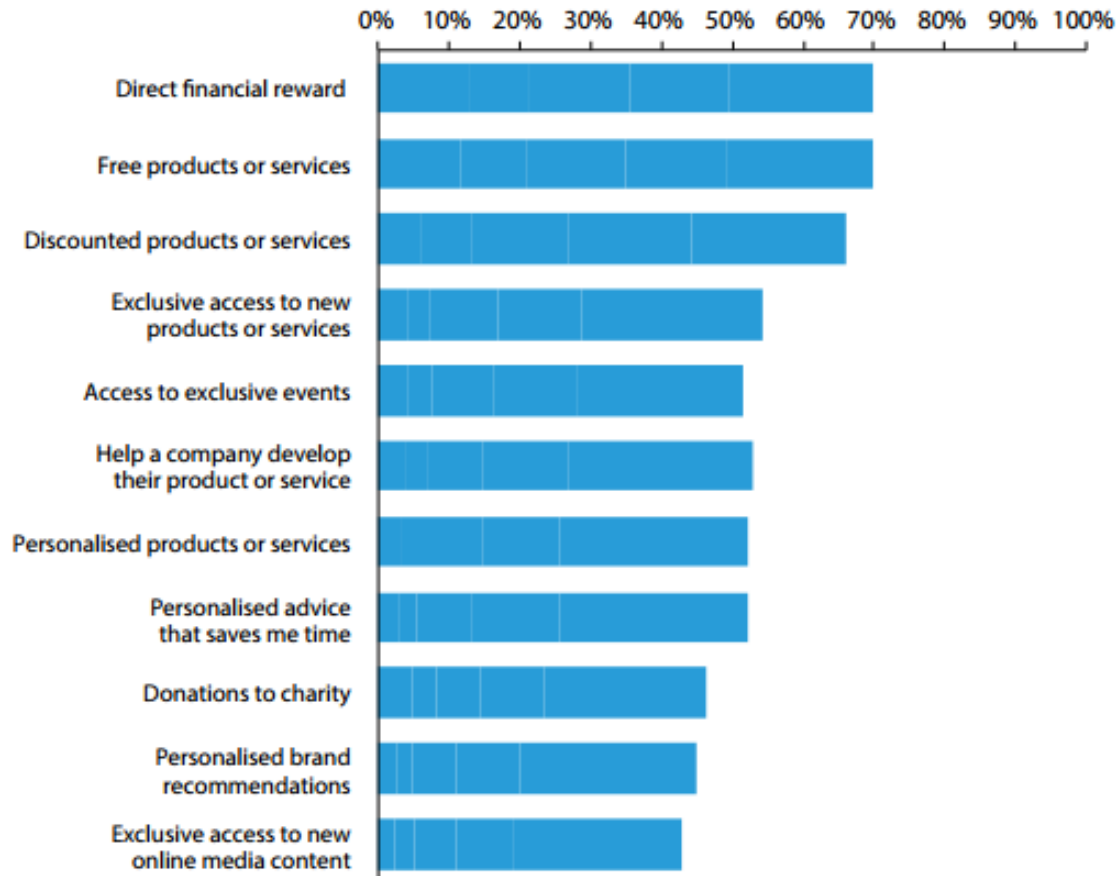


“I see my personal information as an asset that I can use to negotiate better prices and offers with companies” % who strongly agree or agree



Incentives to Exchange Personal Information

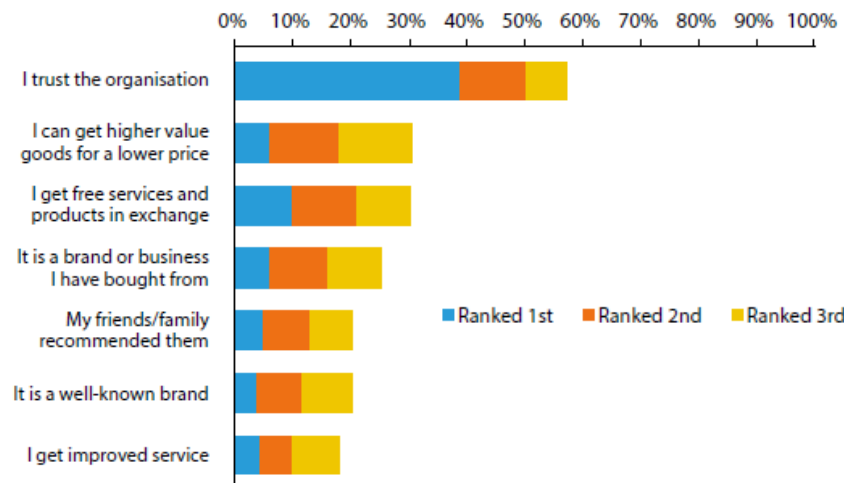
“How likely would you be to share your personal information in exchange for the following incentives? Please use the scale from 1 to 10 where 1 is ‘very likely’ and 10 is ‘not likely at all.’” | % who answer 1-5




The Importance of Trust and Data Stewardship

- Trust continues to be the key element to building a healthy data culture
 - Companies must strive to be good stewards of their customers' data
 - 40% of consumers chose trust in an organization as the most important factor when deciding to share personal information (4x more than next closest)
- Enhancing the consumer's sense of control is paramount
 - 90% of consumers say they want more control over the data they exchange
 - As more consumers strive to manage their own information flow, marketers will be expected to offer more flexible privacy options and to provide them with more autonomy over how their data is collected and used

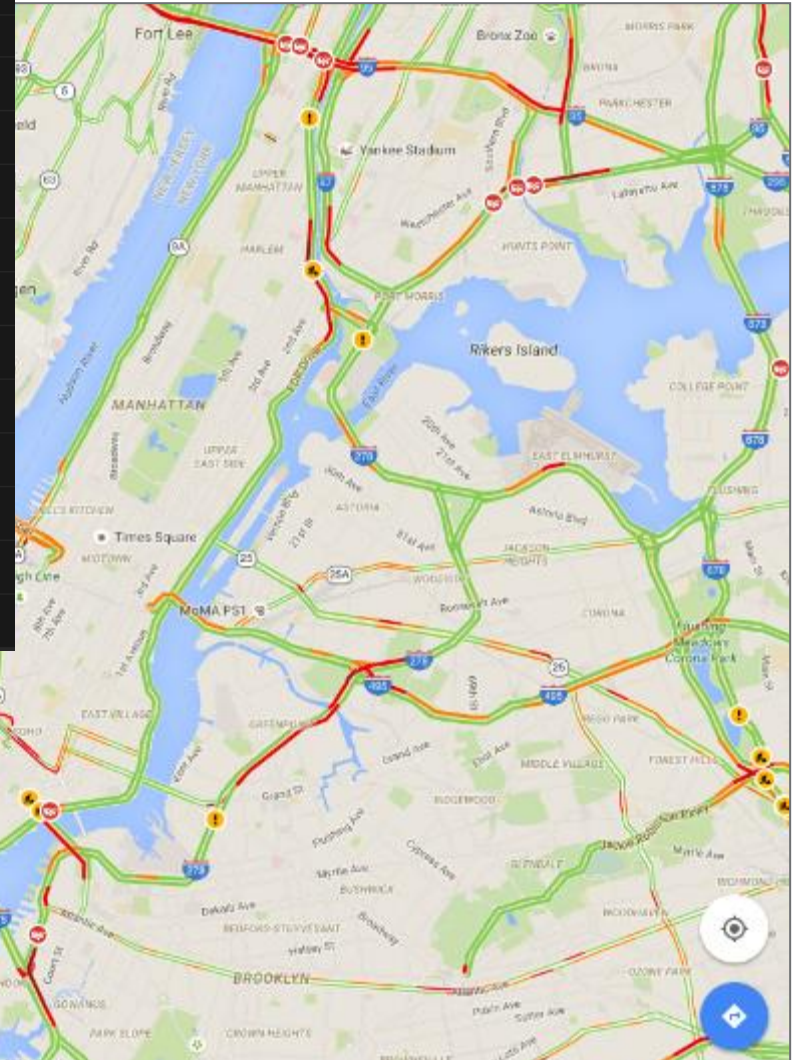
"Please rank the following in terms of what makes you happy to share your personal information with a company?" | % who select each option



Current Real-World Examples of the Benefits of Sharing


Discover Weekly
▶ PLAY

	SONG	ARTIST	ALBUM
+	Melody Day - Four Tet Remix	Caribou, Luke Lalonde, ...	Melody Day (Four Tet Re...
+	Medley: Ike's Rap II/Help Me Love	Isaac Hayes	Black Moses
+	Sit Down	Shazz feat. Michael Robi...	Heritage
+	Dunk	Noiseshaper	Real To Reel
+	State Of Mind	Goldie	Timeless (US DMD)
+	Sleepy Language	Layo & Bushwack!	Night Works
+	Sorry Sorry - Old Skool Afro Dub Re...	Femi Kuti	Shoki Remixed
+	Thinking of Omara	Nightmares On Wax	Mind Elevation
+	Traveller	Talvin Singh	OK (Standard Version)
+	Why Should I Cry	Avia	I See That Now...
+	Beloved - Thievery Corporation Re...	Anoushka Shankar	Rise Remixes
+	Chase Me	Hexstatic	Master-View



Thank You

Ed Brolin
Constellation Energy
on behalf of the Retail Energy Supply Association

212.885.6418 (o)

718.664.3662 (m)

ed.brolin@constellation.com

DOE DATAGUARD FOR SECURE CUSTOMER DATA SHARING

DOE VOLUNTARY CODE OF CONDUCT
CAN ENSURE SECURE DATA SHARING
WITH DER DEVELOPERS

JANUARY 2016

THIRD PARTY DER DEVELOPERS MAY REQUEST ACCESS TO CUSTOMER DATA

Type of Customer Data	Why DER Developers May Request This Data
Individual customer data on location, usage and billing history. This would be opt-in only	To determine which individual customers would be good candidates for DER equipment
Aggregated customer usage data at varying geographic points on feeders	To determine where on the utility feeder to site DER to provide system support while minimizing system impacts
Aggregated customer usage data to a substation	To determine which utility substation could support DER while minimizing system impacts
Average customer billing data by customer class	To perform market research on which customer class would benefit from DER
Hourly daily profiles by customer class, if available	To perform market research on which customer class would benefit from DER

BACKGROUND: HOW DATAGUARD CAN HELP

- Customer data privacy and security remain fundamental objectives as utilities are increasing intelligence on the grid.
- DOE has held workshops and facilitated a 22-month effort to address data privacy concerns and coordinate efforts of all stakeholders.
- On January 12, 2015, President Obama announced the release of the final concepts and principles for a **Voluntary Code of Conduct (VCC)** related to the privacy of customer energy usage data for utilities and third parties.

The final VCC, now branded as the **DataGuard Energy Data Privacy Program**, provides companies with a consumer-facing mechanism to:

- demonstrate their commitment to protecting consumers' data, and thus
- increase consumer confidence.

CODE OF CONDUCT OVERVIEW

The DataGuard Code of Conduct has five core concepts:

- 1 • Customer Notice and Awareness
- 2 • Customer Choice and Consent
- 3 • Data Access and Participation
- 4 • Data Integrity and Security
- 5 • Self-Enforcement Management and Redress

1. CUSTOMER NOTICE AND AWARENESS

- Service-providers should give customers notice about privacy-related policies and practices
 - in easily-understandable formats, clear and conspicuous
 - At start of service, on some recurring basis, and as requested
 - Whenever there is a change in procedure or ownership impacting customer data
- The notice should address:
 - Which specific types of information are being collected, the Primary and Secondary Purpose, and the means of collection
 - How customer data is being used – both aggregate data and individual customer data
 - How customer can access his or her data and request corrections
 - How customer can approve or revoke Third Party access to customer data for a Secondary Purpose
 - How customer data is secured, retained and disposed
 - **Contracted Agents and supporting services with whom the provider is sharing data for Primary Purpose;**
 - **The circumstances under which data will be shared without obtaining customer consent**

2. CUSTOMER CHOICE AND CONSENT

- Service Providers and Contracted Agents require customer data for Primary Purposes. But customers should be able to control Secondary Purpose data sharing. The consent process should:
 - Propose specific data elements to be shared, why, and for how long;
 - Allow customer to authorize or rescind disclosure to Third Parties;
 - Be reasonably secure against fraudulent consent;
 - Allows service provider to charge a fee for custom requests.
- Prior customer consent for data sharing is **not required** in cases of: Third Parties responding to emergencies; Law enforcement; when directed by Federal or State Law; to secure critical infrastructure; or when **data is Aggregated or Anonymized, under contract between Service Provider and Third Parties.**
 - Service Provider will not share with Third Party the customer's: SSN; financial account number; consumer report information; individually identifiable biometric data; or first/last name in combination with any of the following: date of birth; mother's maiden name; electronic signature; DNA profile.

3. CUSTOMER DATA ACCESS AND PARTICIPATION

- Customers should have access to their own Customer Data and be able to participate in its maintenance. This process of participation should:
 - Be reasonably convenient, timely and cost-effective.
 - Allow the customer to identify inaccuracies and request corrections.
 - Allow the Service Provider to charge a fee, to the extent that it offers a method of data access that is different from the method it generally uses or not based on common/standard data formats.
 - Allow the Service Provider to recover costs for Aggregate Data requests that are different from the method it generally uses or not based on common/standard data formats.

4. DATA INTEGRITY AND SECURITY

- Data should be as accurate and complete as reasonably possible given the mode of collection, and securely maintained against unauthorized access.
- Service Provider must mitigate risk through a cyber-security risk management platform which: implements measures to preserve data integrity and prevent loss; maintains a data breach response program; notifies customers of any compromise.

Aggregated Data Methodologies

should consider:

- Customer Identifiers;
- Number of Customers;
- Customer Loads;
- Customer Class;
- Timescale; and
- Geographic Identifiers.

Anonymized Data Methodologies

should consider:

- Customer Identifiers;
- Customer Load;
- Energy Pattern;
- Customer Class;
- Timescale; and
- Masking Data.

5. SELF-ENFORCEMENT MANAGEMENT AND REDRESS

- Service Providers who voluntarily adopt this Voluntary Code of Conduct commit to:
 - Regularly review their Customer Data practices for compliance, accuracy and process improvement;
 - Take action to meet legal and regulatory data protection mandates and ensure compliance with the foregoing concepts;
 - Provide a simple and effective means to address customer concerns. Customer processes should provide timely resolution of customer concerns.
 - Conduct regular training and ongoing awareness activities for relevant employees in the Service Provider organization.

NAVIGANT'S BEST PRACTICES ON CYBERSECURITY



SUMMATION

Navigant supports the adoption of DataGuard because:



DataGuard is aligned with industry best practices on cybersecurity and customer data stewardship.



DataGuard does not negatively impact a Service Provider's ability to provide data to Third Parties, that would allow them to make informed decisions on engaging in DER projects on the distribution grid or on customer sites.

CONTACTS

ERIC SMITH

Managing Director

781.270.8435

Eric.smith@Navigant.com

DAVID O'BRIEN

Director

781.270.8451

David.obrien@Navigant.com

Cyber Security and Privacy Update

DOE Data Guard Program - The *Data Guard Energy Data Privacy Program, Voluntary Code of Conduct, Final Concepts and Principles*

- ❑ Consistent with the DataGuard Program’s core principles:
 - NYSEG and RG&E takes very seriously the job of protecting customers’ privacy; and
 - Privacy and security protections are and will remain fundamental objectives of NYSEG and RG&E .
- ❑ NYSEG and RG&E has reviewed the Voluntary Code of Conduct (“VCC”)and believes that the VCC is in line with industry best practices;
- ❑ NYSEG and RG&E is already working towards many of the goals and concepts outlined in the VCC;
- ❑ NYSEG and RG&E finds significant value in the identification of best practices for the industry as a whole to follow;
 - Accordingly, IUSA believes that the most beneficial course of action for NYSEG and RG&E , its investors and customers is to commit to adopt DataGuard.

Cyber Security and Privacy Update

DOE Data Guard Program - *The Data Guard Energy Data Privacy Program, Voluntary Code of Conduct, Final Concepts and Principles*

RG&E and NYSEG have addressed or are working toward addressing DataGuard's five high level principles in the following ways:

- Customer Notice and Awareness-** The concept that customers should be given notice about privacy-related policies and practices as part of providing service.
 - RG&E and NYSEG currently has a privacy statement and terms and conditions/legal disclaimer on our website as well as Corporate Governance that includes Global Policies including Personal Data Protection Policy.
- Customer choice and Consent-** The concept that customers should have a degree of control over access to their Customer Data
 - RGE and NYSEG provide customers access to their data through the online portal as well as by contact customer service.
 - We agree that consent should be opt-in , which we are starting to address through updated notices as well as more definitive methods to provide consent moving forward.
 - With opt-in consent, we are working toward this requirement, but given current state with REV initiatives we are unable to achieve given the data (aggregated) that is being requested for the projects.
 - We want to be able to educate and provide openness and transparency for our customer so they understand how their data is being collected, processed, disclosed and retained, in the short term and long term.
- Customers data access and participation-**The concept that customers should have access to their own customer data and should have the ability to participate in its.
 - RG&E and NYSEG customers have the ability to access their own data by making changes online and/or by contacting customer service for any potential discrepancies.
- Integrity and Security-**The concept that Customer Data should be as accurate as reasonably and possible, and secured against unauthorized access.
 - RG&E and NYSEG have a robust Cyber Security Framework that is built on ISO 27001 and 27002, with multiple global rules that address Cyber Security. Cybersecurity and privacy go hand in hand as you cannot have Privacy without Security.
 - Global rules include Global Asset Management Rule, Information Asset Classification Rule and Framework that align with our Privacy Impact Assessments, Records Retention and Management and Incident Response an Management Rule
 - Third Party Risk Assessments and Contractual language with vendors and third parties: Data Security Riders and Cyber Insurance
- Self Enforcement Management and Redress-** The concept that there should be enforcement mechanisms to ensure compliance with the foregoing concepts and principles.
 - We have a Privacy training department that leads ongoing training.
 - Annual Cyber Security conference that is attended by all levels of management and provider training and awareness to our business security liaisons.
 - Global policies and rules are reviewed on a regular basis and are approved by our Global Cybersecurity committee

Cyber Security and Privacy Update

DOE Data Guard Program - The Data Guard Energy Data Privacy Program, Voluntary Code of Conduct, Final Concepts and Principles

- ❑ NYSEG and RG&E finds significant value in the identification of best practices for the industry as a whole to follow;
 - Accordingly, IUSA believes that the most beneficial course of action for NYSEG and RG&E , its investors and customers is to commit to adopt Data Guard.
 - Commitment to educating our customers.
 - Commitment to ensuring our customers understand how their information is collected, processed, disclosed and retained.
 - Commitment to brand integrity through open and transparent communications customers, leading to trust.
 - Commitment to implementing robust security measures that protect the confidentiality, integrity and ability of our customers information.
 - Align with state and federal regulations.
 - Align with industry best practices such as GAPP, OECD as well as FTC and the draft Cybersecurity framework being created for the PSC by the JUs.

UtilityAPI <> DataGuard VCC Presentation

Daniel Roesler, Co-founder & CTO, UtilityAPI
NY REV Conference, January 20, 2016

UtilityAPI Background

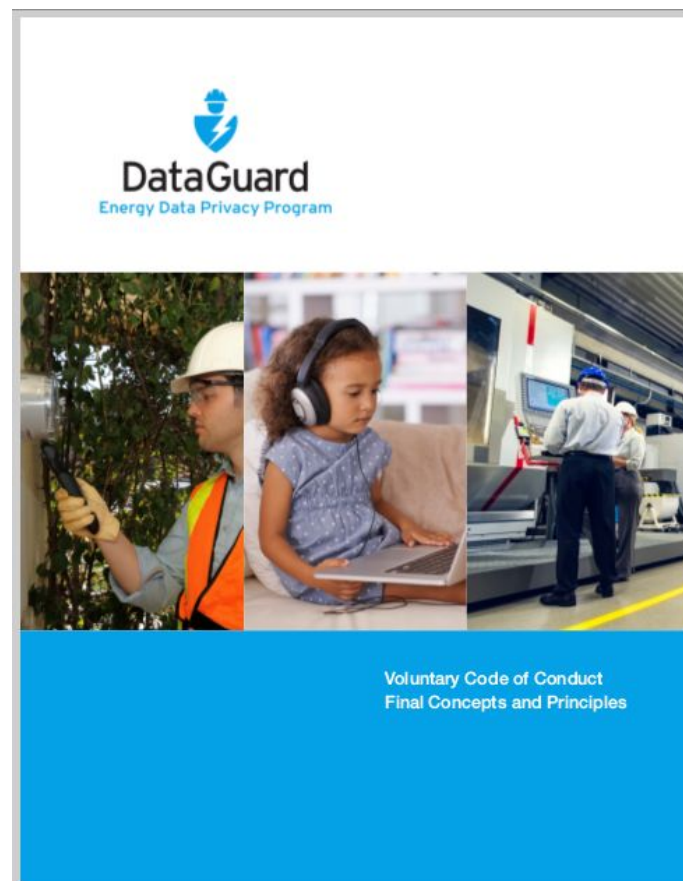
- Energy data infrastructure, authorization, and communication company
- Builds connections between utilities, account holders, and third parties
- Works with many solar, energy efficiency, and building management
- Submitted official adoption statement for DataGuard VCC
- Green Button Alliance member and active participant
- Department of Energy Sunshot Catalyst and Incubator Awardee
- Hawaii Energy Excelerator Awardee
- Specializes in direct customer authorization and streamlined consent



DOE DataGuard Voluntary Code of Conduct (VCC)

Two main focuses:

1. Customer authorization
2. Data handling and security



UtilityAPI Customer Authorization Recommendations

1. Always require customer opt-in and consent, for both individual and aggregate data sharing.
2. Recognize that the authorization process is usually just one step in a multi-step energy analysis, audit, or quote process. Focus on simplified and clear user experience. Use best practices, don't try and reinvent the wheel.

DataGuard VCC Data Definitions

Types of customer energy data:

1. Customer Energy Use Data (CEUD) (intervals, etc.)



VCC says can be anonymous

2. Account Data (service address, meter number, etc.)



VCC says is personally identifiable

UtilityAPI Data Handling Recommendations

1. Consider all individual data (including CEUD) as personally identifiable. It's very difficult to anonymize individual data, and CEUD alone isn't very useful anyway.
2. If need anonymous data, aggregate it. However, we still recommend opt-in consent from customer.
3. Encrypt data and communications. Require HTTPS for websites that serve individual customer energy data.
4. Keep customer energy data inside the United States.

UtilityAPI Summary Recommendations

- DataGuard is a good minimum, but should have additions:
 - Always require customer opt-in, even for aggregated
 - Focus on user experience and easy authorization
 - Treat individual customer data (including CEUD) as PII
 - Anonymous data should only be aggregated data
 - Encrypt data and communications
 - Keep customer data inside the United States

**Thanks! Please
come talk to us!**

Daniel Roesler
daniel@utilityapi.com