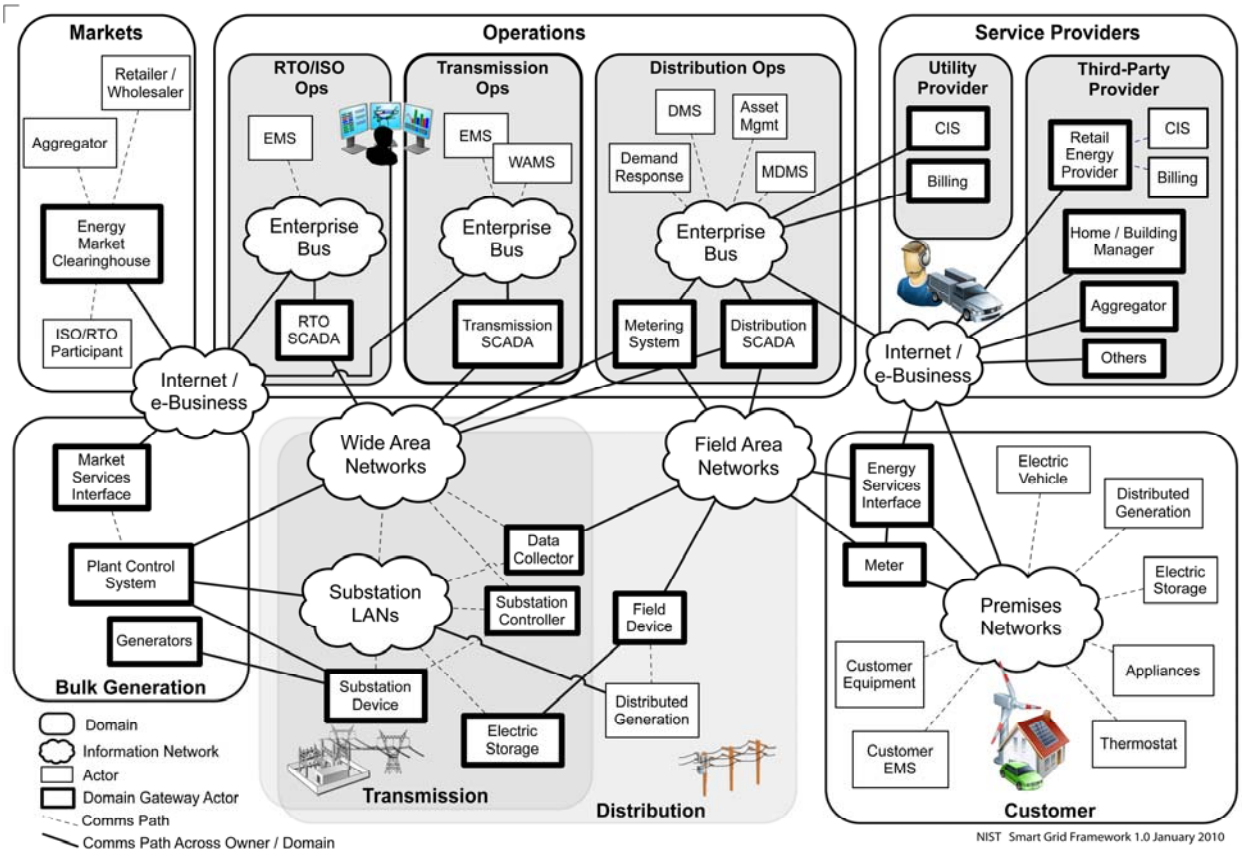

Figure 5-2 NIST Conceptual Model [37]

The proliferation of smart appliances, utility devices, and devices from other entities throughout the Smart Grid, on both sides of the meter, means an increase in the number of devices that may generate data. The privacy risks presented by these smart appliances and devices on the consumer side of the meter are expanded when these appliances and devices transmit data outside of the home area network (HAN) or energy management system (EMS) and do not have documented security requirements, effectively extending the perimeter of the system beyond the walls of the premises.

Data may also be collected from plug-in electric vehicles (PEVs). Charging data may be used to track the travel times and locations for the PEV owners.

5.4 CONSUMER-TO-UTILITY PRIVACY IMPACT ASSESSMENT

A PIA is a comprehensive process for determining the privacy, confidentiality, and security risks associated with the collection, use, and disclosure of personal information. PIAs also define the measures that may be used to mitigate and, wherever possible, eliminate the identified risks. The Smart Grid PIA activity provides a structured, repeatable type of analysis aimed at determining how collected data can reveal personal information about individuals or groups of individuals, and the focus of the PIA can be on a segment within the grid or the grid as a whole. Privacy risks

[37] *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.* Available at http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

Table 5-2 Potential Privacy Concerns and Descriptions

Privacy Concern	Discussion	Categorization
Fraud	Attributing energy consumption to another location or vehicle (in the case of PEVs).	Type II: While fraud is an existing concern, the current system of reading consumer meters (either manual recording or electronically via "drive-by" remote meter reading systems) may allow less opportunity for data manipulation without collusion with the personnel collecting the data.
Determine Personal Behavior Patterns / Appliances Used	Smart meter and home automation network data may track the use of specific appliances. Access to data-use profiles that can reveal specific times and locations of electricity use in specific areas of the home can also indicate the types of activities and/or appliances used. Possible uses for this information include: Appliance manufacturers could use this information for product reliability and warranty purposes; Other entities could use this data to do targeted marketing.	Type I: The type of data made available by Smart Grid implementation may be both more granular and available on a broader scale.
Perform Real-Time Remote Surveillance	Access to live energy use data can reveal such things as if people are in a facility or residence, what they are doing, waking and sleeping patterns, where they are in the structure, and how many are in the structure.	Type II: Many methods of real-time surveillance currently exist. The availability of computerized real-time or near-real-time energy usage data would create another way in which such surveillance could be conducted.
Non-Grid Commercial Uses of Data	Personal energy consumption data storage may reveal lifestyle information that could be of value to many entities, including vendors of a wide range of products and services. Vendors may purchase attribute lists for targeted sales and marketing campaigns that may not be welcomed by those targets. Universities might purchase information to study student attributes and target a new student profile with simple application question profiling. Such profiling could extend to other types of profiling on employment selection, rental applications, and other situations that may not be welcomed by those targets.	Type II: Under the existing metering and billing systems, meter data is not sufficiently granular in most cases to reveal any detail about activities. However, smart meters, time of use and demand rates, and direct load control of equipment may create detailed data that could be sold and used for energy management analyses and peer comparisons. While this information has beneficial value to third parties, consumer education about protecting that data has considerable positive outcomes.

the data, and that they consider these factors when developing processes for data collection, handling, and disclosure.

Many potential uses arise from the generation of granular energy data, especially when it is combined with personal information. Table 5-3 broadly illustrates the various industries that may be interested in Smart Grid data. While this is not an exhaustive listing, it serves to help categorize the various concerns.

Table 5-3 Potential Privacy Impacts that Arise from the Collection and Use of Smart Grid Data

Type of Data	Privacy-Related Information Potentially Revealed by this Type of Data	Parties Potentially Collecting or Using this Type of Data	Type of Potential Use[61]	Specific Potential Uses of this Type of Data
Captures detailed energy usage at a location, whether in real-time or on a delayed basis.	*Personal Behavior Patterns and Activities Inside the Home* Behavioral patterns, habits, and activities taking place inside the home by monitoring electricity usage patterns and appliance use, including activities like sleeping, eating, showering, and watching TV. Patterns over time to determine number of people in the household, work schedule, sleeping habits, vacation, health, affluence, or other lifestyle details and habits. When specific appliances are being used in a home, or when industrial equipment is in use, via granular energy data and appliance energy consumption profiles. *Real-Time Surveillance Information* Via real-time energy use data, determine if anyone is home, what they are doing, and where they are located in the home.	Utilities	Primary	Load monitoring and forecasting; demand response; efficiency analysis and monitoring, billing.
		Edge Services[62]		Efficiency analysis and monitoring; demand-response, public or limited disclosure to promote conservation, energy awareness, etc. (e.g., posting energy usage to social media).
		Insurance Companies	Secondary	Determine premiums (e.g., specific behavior patterns, like erratic sleep, that could indicate health problems).
		Marketers		Profile for targeted advertisements.
		Law Enforcement		Identify suspicious or illegal activity; investigations; real-time surveillance to determine if residents are present and current activities inside the home.
		Civil Litigation		Determine when someone was home or the number of people present.
		Landlord/Lessor		Use tenants' energy profiles to verify lease compliance.
		Private Investigators		Investigations; monitoring for specific events.
		The Press		Public interest in the activities of famous individuals.[63]

[61] "Primary" uses of Smart Grid data are those used to provide direct services to customers that are directly based on that data, including energy generation services or load monitoring services. "Secondary" uses of data are uses that apply Smart Grid data to other business purposes, such as insurance adjustment or marketing, or to nonbusiness purposes, such as government investigations or civil litigation. "Illicit" uses of data are uses that are never authorized and are often criminal.

[62] Edge services include businesses providing services based directly upon electrical usage but not providing services related to the actual generation, transportation, or distribution of electricity. Some examples of edge services would include Google PowerMeter, Microsoft Hohm, or consulting services based upon electricity usage.

Type of Data	Privacy-Related Information Potentially Revealed by this Type of Data	Parties Potentially Collecting or Using this Type of Data	Type of Potential Use[61]	Specific Potential Uses of this Type of Data
		Creditors		Determine behavior that seems to indicate creditworthiness or changes in credit risk.[64]
		Criminals and Other Unauthorized Users	Illicit	Identify the best times for a burglary; determine if residents are present; identify assets that might be present; commit fraud; identity theft; disrupt service; corporate espionage—determine confidential processes or proprietary data.
Identifies location / recharge information for PEVs or other location-aware appliances.	*Determine Location Information* Historical PEV data, which can be used to determine range of use since last recharge. Location of active PEV charging activities, which can be used to determine the location of driver.	Utilities	Primary	Bill energy consumption to owner of the PEV; distributed energy resource management; emergency response.
		Insurance Companies	Secondary	Determine premiums based on driving habits and recharge location.
		Marketers		Profile and market based on driving habits and PEV condition.
		Private Investigators Law Enforcement/ Agencies		Investigations; locating or creating tracking histories for persons of interest.
		Civil Litigation		Determine when someone was home or at a different location.
		PEV Lessor		Verify a lessee's compliance regarding the mileage of a lease agreement.
Identifies individual meters or consumer-owned equipment and	*Identify Household Appliances* Identifying information (such as a MAC address); directly reported usage information provided by	Utilities	Primary	Load monitoring and forecasting; efficiency analysis and monitoring; reliability; demand response; distributed energy resource management; emergency response.

[63] For example, there were numerous news stories about the amount of electricity used by Al Gore's Tennessee home. *See* e.g., "Gore's High Energy-Use Home Target of Critical Report," Fox News, Feb. 28, 2007, available at http://www.foxnews.com/story/0,2933,254908,00.html.

[64] Sudden changes in when residents are home could indicate the loss of a job. Erratic sleep patterns could indicate possible stress and increased likelihood of job loss. *See e.g.*, Charles Duhigg, "What Does Your Credit-Card Company Know About You?" NY Times Mag., May 17, 2009 MM40, available at http://www.nytimes.com/2009/05/17/magazine/17credit-t.html.

Type of Data	Privacy-Related Information Potentially Revealed by this Type of Data	Parties Potentially Collecting or Using this Type of Data	Type of Potential Use[61]	Specific Potential Uses of this Type of Data
capabilities.	"Smart" appliances. Data revealed from compromised smart meter, HAN, or other appliance.	Edge Services		Efficiency analysis and monitoring; broadcasting appliance use to social media.
		Insurance Companies	Secondary	Make claim adjustments (e.g., determine if claimant actually owned appliances that were claimed to have been destroyed by house fire); determine or modify premiums based upon the presence of appliances that might indicate increased risk; identify activities that might change risk profiles.
		Marketers		Profile for targeted advertisements based upon owned and unowned appliances or activities indicated by appliance use.
		Law Enforcement		Substantiate energy usage that may indicate illegal activity; identify activities on premises.
		Civil Litigation		Identify property; identify activities on premises.
		Criminals & Other Unauthorized Users	Illicit	Identify what assets may be present to target for theft; disrupt operation of appliances or electric service; introduce a virus or other attack to collect personal information or disrupt service; compromise smart meters to steal energy.[65]

Such data might be used in ways that raise privacy concerns. For example, granular Smart Grid data may allow numerous assumptions about the health of a dwelling's resident in which some insurance companies, employers, newspapers (when regarding public figures), civil litigants, and others could be interested. Most directly, specific medical devices may be uniquely identified through serial numbers or MAC addresses, or may have unique electrical signatures; either could indicate that the resident suffers from a particular disease or condition that requires the device.[66]

[65] See Matthew Carpenter et al., "Advanced Metering Infrastructure Attack Methodology" pages 55-56 (Jan. 5, 2009), available at http://inguardians.com/pubs/AMI_Attack_Methodology.pdf (discussing how attackers could manipulate the data reported to utilities); Robert Lemos, "Hacking the Smart Grid", Tech. Rev. (Apr. 5, 2010), available at http://www.technologyreview.com/printer_friendly_article.aspx?id=24977&channel=energy&section=.

[66] Susan Lyon & John Roche, Smart Grid News, "Smart Grid Privacy Tips Part 2: Anticipate the Unanticipated" (Feb. 9, 2010), available at