Ranking Electricity Meters for Risk to Health, Privacy, and Cyber Security

Introduction

The manufacturers of electricity meters offer a wide variety of models. And many of these models are available with a dozen or so options, leading to an enormous number of possible combinations. These meters have capabilities beyond what is required to measure the electricity consumed for the purpose of issuing a monthly bill. Unfortunately, the new capabilities present a host of risks to health, to privacy, and to cyber security, as has been widely discussed elsewhere. But, briefly --

- The risks to health arise primarily from the fact that many electricity meters communicate wirelessly with the electric power companies. They transmit radiofrequency radiation, at microwave frequencies, day and night, every day of the year, forever. That radiation travels through homes and businesses readily, and penetrates the unborn, the children, and the adults alike, disrupting health. Every transmitting meter in a community irradiates everyone in that community. So does every community-based transmitter/receiver that the electric power companies have erected to communicate wirelessly with those meters.

- The risks to privacy arise from the fact that many of the meters capture and transmit very highly time-resolved information about electricity consumption. That detailed information can reveal much about the activities taking place inside the homes and the businesses, sufficient, for example, to reveal when no one is there.

- The risks to cyber security arise, in part, from the fact that some types of meters can accept incoming wireless commands that may come from nefarious sources. Many of those meters can respond to wireless commands to shut off the electrical power to a home or a business entirely, or to accept new software programming. That new programming can alter the functions of the meters and can do so invisibly to the owners of the homes and the businesses.

[1] Ronald M. Powell is a retired career U.S. Government scientist who holds a Ph.D. in Applied Physics from Harvard University. During his Government career, he worked for the Executive Office of the President, the National Science Foundation, and the National Institute of Standards and Technology.

The variety of meters now in service, and the many risks that the meters can pose, mean that it has become impossible for the customer of an electric power company to know what capabilities his meter has and what risks those capabilities imply for him, his family, his business, and his community. In short, the electric power companies have moved --

- *from* the accepted practice of measuring electricity consumption once a month for the purpose of issuing a proper monthly bill
- *to* the questionable practice of monitoring the daily activities inside individual homes and businesses, as reflected in their detailed patterns of electricity consumption
- *then* broadcasting those details over the air using wireless technology that pollutes entire communities with hundreds of millions of bursts of microwave radiation every day, forever.

Purpose of this Document

The purpose of this document is to provide some perspective about the types of meters available and the relative risks that they pose. Because there are so many types of meters available, not all of them could be addressed here. The meters selected for this document are those that I have seen in service most often in my state of Maryland, and those that offer the greatest potential for reducing risk to health, privacy, and cyber security.

Principal Conclusions

Only one type of meter, the Traditional Analog Mechanical Meter with No Wireless Communications Capability, represented by the last row in Figure 1 on page 6, offers ***all*** three of the following positive characteristics:

- no risk to health from RF radiation exposure, because it generates no RF radiation
- no risk to privacy, because it cannot be remotely read
- no risk to cyber security, because it cannot be remotely accessed so it cannot be hacked.

In sum, the meter that poses the lowest risk to health, to privacy, and to cyber security is the Traditional Analog Mechanical Meter with No Wireless Communications Capability. Tragically, this is the meter that many electric power companies in Maryland have chosen to remove.

Only one type of meter examined here, the Wireless Smart Meter, represented by the first row in Figure 1 on page 6, has ***all*** three of the following negative characteristics:

- the highest risk to health because it has the highest Peak Radiofrequency (RF) Power Output, and because it has either the first or the second highest number of bursts of RF radiation per day, depending on its operating mode

- the highest risk to privacy because its data are potentially accessible to the second largest number of people, but with the greatest ease of access to the data stream (because it is wireless), and because it provides data with the greatest timeliness, the greatest granularity (finest time-resolution), and the greatest variety (most types of data), all of which make that data highly intrusive

- the highest risk to cyber security because it is potentially accessible to the second largest number of people, but again with the greatest ease of access (because it is wireless), and because it is the most vulnerable to being harmed itself, and because it is the most able to cause harm

    - because it contains a shutdown switch capable of shutting off all power to the customer when triggered to do so by a wireless remote signal

    - because it is software reprogrammable to perform new functions, whether beneficial or harmful, entirely invisibly to the customer.

In sum, the meter that poses the highest risk to health, to privacy, and to cyber security is the Wireless Smart Meter. Tragically, this is the meter that many electric power companies in Maryland have chosen to install.

The other meters discussed in this document fall somewhere in between the above two meters.

- All of these other meters pose a risk to health from RF radiation exposure, although to widely differing degrees.
- All but one of those other meters pose a risk to privacy.
- Two of those other meters pose a risk to cyber security.

Organization of this Document

The rest of this document is organized as follows:

Ranking Electricity Meters for Risk to Health

Figure 1 on page 6 ranks electricity meters for their risk to health, based on the characteristics of the "Sources of Radiofrequency (RF) Radiation" that the meters contain. All of the terms used in the figure are described in the text that immediately follows the figure.

The rows in the figure name the "Meter Category" into which each meter falls and the "Type of Communication", whether wireless or wired, that each meter employs. In the central part of the figure, the column headings and subheadings describe the "Sources of Radiofrequency (RF) Radiation" in each meter and the characteristics that those sources have that are of relevance to their risk to health. The presence of a red cell in a given row and column means that the meter described in the heading of that row employs the RF radiation source described in the heading of that column and poses a risk to health.

The first of the column subheadings indicates the "Peak RF Power Output" of each RF source. Note that the sources are arranged, from left to right, from the lowest to the highest levels of Peak RF Power Output. Peak RF Power Output is one of the most important factors

affecting the risk to health. The higher the Peak RF Power Output, if other factors are equal, the more RF radiation is being delivered and the higher the associated risk to health.

The second of the column subheadings indicates the number of "Bursts of RF (Radiation) per Day" or per month, if known, issued by each Source of RF Radiation. The higher the number of Bursts of RF Radiation per Day, the more RF radiation is being delivered and the higher is the associated risk to health.

The last column on the right side of Figure 1, labelled "Overall Risk", shows a numeric ranking for the "Risk to Health", for each row, that is for a given meter with a given type of communication. The higher that number, the higher is the associated risk to health. All of the numbers in the red cells under "Risk to Health" indicate a *rank order*. That is a Rank 5 meter presents more risk to health than a Rank 4 meter. Rank 5 represents the highest risk, and a blank cell represents the lowest risk. Note that the rankings are not quantitative beyond the order that they indicate. That is, the rankings do not indicate *how much a given meter differs from another*. The quantitative difference is better judged by examining the differences in Peak RF Power Output and in Bursts of RF per Day, where those numbers have been provided. In some cases, I did not have good numbers to offer; but I still made an educated, but only qualitative, guess, such as "very low" or "high". The purpose was to indicate the range into which I would expect the actual numbers, if known, to fall. I flagged each such entry as "unknown".

Note that no meter in Figure 1 has Risk 1. That is largely because every electricity meter, except the Traditional Analog Mechanical Meter with No Wireless Communications Capability, has at least two sources of RF Radiation, both of which are very busy generating RF radiation even if at a very low Peak RF Power Output. Only one meter, the Traditional Analog Mechanical Meter with No Wireless Communications Capability, has no sources of RF radiation, and thus merits a blank for Risk to Health, indicating that it is clearly the safest meter for health of them all.

Figure 1: Ranking Electricity Meters for Risk to Health

(RED means "generates radiofrequency radiation at a level potentially risky to health".)

Meter Category ↓	Type of Communication ↓			Sources of Radiofrequency (RF) Radiation in Meter						Overall Risk 5 is highest. Blank is lowest.
				Unintentional Radiators		Intentional Radiators (transmitters)				
				Digital Electronics	Switching Power Supply	Not Networked Transmitter/Receiver		Home Area Network (HAN) Transmitter/Receiver	Wide Area Network (WAN) Transmitter/Receiver	
	Peak RF Power Output →			*very low (unknown)*	*very low (unknown)*	*low (1 mW)*	*low to medium (1-100 mW)*	*medium (100 mW)*	*high (1000 mW)*	
	Bursts of RF per Day →			*high (unknown)*	*high (unknown)*	*low (8 per month)*	*high (50,000 per day)*	*high (unknown)*	*high [10,000 (avg) to 190,000 (max) per day]*	**Risk to Health**
		wireless	*wired*							
SMART METER Digital Advanced Metering Infrastructure (AMI)	**WAN/ HAN**	✓								**5**
	Internet cable/fiber		✓							**2**
	Telephone landline		✓							**2**
Digital Automated Meter Reading (AMR)	**Bubble Up**	✓								**4**
	Wake Up	✓								**3**
	Internet cable/fiber		✓							**2**
	Telephone landline		✓							**2**
Basic Digital Electronic Meter	**None**									**2**
Analog Meter (plus wireless digital electronics)	**Bubble Up**	✓								**4**
	Wake Up	✓								**3**
Traditional Analog Meter	**None**									

Description of Electricity Meters

Meter Categories

A **Smart Meter** is the key component in what is called the **Advanced Metering Infrastructure (AMI)**. As a result, Smart Meters are often referred to as AMI Meters. The Smart Meter is a digital electronic device that monitors the flow of electricity into, and out of, a customer's residence or business and provides two-way communication between the customer's meter and the electric power company. The information sent to the electric power company describes many characteristics of that flow of electricity, and on a very timely and highly time-resolved ("granular") basis. That communication is usually accomplished with a **wireless** transmitter/receiver, called a Wide Area Network (WAN) because it has a high enough Peak RF Power Output to travel great distances. It is this WAN which gives rise to most of the health concerns about Smart Meters, while simultaneously heightening both the privacy and the cyber-security concerns, both because of the wide area covered by the signals and because of the accessibility of any signal sent through the air.

Each Smart Meter can be, and usually is, equipped with a second **wireless** transmitter/receiver, called a Home Area Network (HAN), to communicate wirelessly with individual so-called Smart Appliances located inside a home or a business, further heightening health, privacy, and cyber-security concerns. The HAN is intended to return to the electric power company information on the identity and the use of each Smart Appliance in a home or business. Whether the HAN can also enable the electric power company to control those Smart Appliances is unknown to me.

Communication between Smart Meters and electric power companies can also be accomplished with **wired** technologies, such as telephone landlines and Internet connections (cable or fiber), which significantly reduce the radiation exposure produced by the Smart Meters, but do not eliminate it entirely. Wired communications for Smart Meters are not employed in Maryland, as far as I know. As an example of a **wired** installation, fiber optic cable is employed in Chattanooga, Tennessee to communicate with that town's Smart Meters.[2]

The digital **Automated Meter Reading (AMR)** meter is another category of digital electronic device that monitors the flow of electricity into, and out of, a customer's residence, but not usually at as high a level of detail as a Smart Meter. The AMR meter can provide **wireless** communication but not usually directly back to the electric power company. Rather, the AMR meters communicate wirelessly with a passing utility vehicle (drive-by reader) or with a passing meter reader on foot (walk-by reader), each equipped with

[2] Your Gig is Here. Right here, in Chattanooga (http://www.chattanoogagig.com/). How Chattanooga beat Google Fiber by half a decade, The Washington Post, September 17, 2013. (http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/17/how-chattanooga-beat-google-fiber-by-half-a-decade/).

the electronic equipment needed to communicate with the AMR meter. Because the distance over which the AMR meter must communicate is shorter than that of a Smart Meter, the Peak RF Power Output of an AMR meter is usually less than that of a Smart Meter. Two different types of wireless communications are offered: Bubble Up and Wake Up. They are described on page 9. If equipped with the proper options, AMR meters can also communicate through wired Internet connections (either cable or fiber optic) or through telephone landlines. Either of these latter two approaches enables communication all the way back to the electric power company, so no drive-by or walk-by meter reader is required.

A **Basic Digital Electronic Meter** is the simplest of all digital electronic meters. It does not employ any wireless or wired communications technology. Such meters are read by a walk-by meter reader who must enter the customer's property. These meters have just two sources of RF radiation -- digital electronics and switching power supply -- so they pose a lower risk to health than some of the other meters. These meters may be able to store a very large amount of data collected between readings by the walk-by meter reader, depending on the options (such as additional electronic memory) that they contain, which may raise some privacy concerns. And that data may be readable very quickly through an electronic or optical interface that the walk-by meter reader connects to the meter. But because such included capability is optional and because these meters are read infrequently (once a month typically), I have ranked these meters as having no risk to privacy. These meters pose no risk to cyber security, either, since they cannot be remotely accessed and therefore cannot be hacked.

An **Analog Meter (plus wireless digital electronics)** is a Traditional Analog Mechanical Meter or, equivalently, a Traditional Analog *Electromechanical* Meter, to which has been added digital electronic circuits, powered by a switching power supply, to give the meter wireless Wake-Up or wireless Bubble-Up communications capability. These capabilities are discussed further on page 9. They enable the meter to be read remotely from a short distance by a drive-by or a walk-by meter reader so that the meter reader does not have to enter the customer's property.

The **Traditional Analog Mechanical Meter with no Wireless Communications Capability** or, equivalently, the Traditional Analog *Electromechanical* Meter with No Wireless Communications Capability, is what is usually meant when the shorter descriptions -- Analog Meter, or Analog Mechanical Meter, or Analog Electromechanical Meter -- are used. This meter contains no digital electronic circuits and thus needs no switching power supply to power those circuits. This type of meter contains no sources of RF radiation, whether intentional or unintentional, and thus does not give rise to a risk to health from exposure to RF radiation. This type of meter also poses no risk to privacy because it cannot be remotely read, and it poses no risk to cyber-security because it cannot be remotely accessed and therefore cannot be hacked. This result is reflected in the blank cells across the bottom row of Figure 1 and the bottom row of Figure 2, reflecting the fact that this meter is the safest one available with regard to risk to health, privacy, and cyber security.

Sources of Radiofrequency (RF) Radiation

All of the sources of RF radiation in electricity meters can radiate directly into the air. Those sources can also deliver RF electrical current directly into the house wiring, or they can induce RF electrical current in the house wiring, which then can radiate into the air. The sources of radiation are described below in order of increasing Peak RF Power Output. While the sources are of widely different levels, even the least powerful of them, the "Unintentional Radiators", can disrupt highly sensitive individuals and thus cannot be ignored.

Unintentional Radiators are sources of radiofrequency radiation that radiate because of their inherent nature, not because the radiation is needed to perform a communications function.

> **Digital Electronics** operate by turning the flow of electrical current on and off sharply and rapidly. These transitions in current flow produce unintentional radiofrequency radiation, whether or not the same electronics also produce intentional radiofrequency radiation for wireless communication. This unintentional radiation is likely lower in Peak RF Power Output, and higher in frequency, than the unintentional RF radiation from Switching Power Supplies.
>
> **Switching Power Supplies** convert the high incoming line voltage from the electrical power system to the lower voltages required to power digital electronic circuits. In this conversion process, these supplies turn the flow of electrical current on and off sharply and rapidly. These transitions in current flow produce unintentional radiofrequency radiation. This unintentional radiation is likely higher in Peak RF Power Output, and lower in frequency, than the unintentional RF radiation from Digital Electronics. (Switching power supplies are also called switched-mode power supplies or switching-mode power supplies.)

Intended Radiators are sources of radiofrequency radiation that must radiate to perform their intentional function, which in this case is the transmission of information in a wireless communication system.

> The **Not Networked Transmitter/Receiver** category includes both the Bubble-Up and the Wake-Up types of communication for electricity meters. Together these two types of communication are sometimes called "encoder, receiver, transmitter" or "ERT" communications. The meters are not linked together in a network.
>
> > **Bubble-Up** meters send their meter readings as wireless signals every second or so, all day and all night long, every day of the year. The purpose of such frequent transmissions is to assure that a signal is available whenever a drive-by or a walk-**b**y employee of the electric company passes with electronic equipment that can pick up and store the information carried by that signal. Bubble-Up meters are offered with Low and Medium Peak RF Power Outputs. I have not yet

learned whether some Bubble-Up meters have a receiver for a different purpose, such as to accept changes in their internal programming.

Wake-Up meters contain receivers that listen for a wireless signal (a "Wake-Up" signal) transmitted by a drive-by or a walk-by meter reader and then respond with a series of transmissions that contain the meter's information. Eight such transmissions, one immediately after the other, appear common. The Wake-Up meters do not transmit at all in between such wake-up signals. As far as I can determine, Wake-Up meters operate only at Low Peak RF Power Output. Because of their infrequent transmissions and their Low Peak RF Power Output, Wake-Up meters produce much less radiofrequency radiation than Bubble-Up meters.

A **Home Area Network (HAN) Transmitter/Receiver** is one of two wireless methods of two-way communication that is usually, but not always, included in Wireless Smart Meters. The HAN is sometimes called the Zigbee Network, after the technology on which it is based. The HAN is designed to communicate with emerging so-called Smart Appliances inside each home or business. The purpose is to monitor those appliances and to transfer information about their identity and their use back to the electric power company. It is possible, but not yet clear to me, that the HAN will enable the electric power companies to exert a degree of remote control over Smart Appliances. The HAN transmits RF radiation (at microwave frequencies) with a Medium Peak RF Power Output. I have not yet found data on how often the HAN transmits its bursts of RF radiation, but I suspect that the burst rate will be high, like that of other types of local area networks (LANs). Depending on that answer, the radiation produced by the HAN may rival or exceed the radiation produced by the WAN.

A **Wide Area Network (WAN)** is a wireless method of two-way communication for Smart Meters and usually takes the form of a so-called Mesh Network. The WAN transmits RF radiation (at microwave frequencies) at a High Peak RF Power Output and thus has considerable range, hence the "wide" in Wide Area Network. In such a network the Smart Meters communicate with each other constantly. Each Smart Meter sends information about the use of electricity in the home or the business that it primarily serves. Each Smart Meter also relays information from the Smart Meters of neighboring homes and businesses. This relay action helps to assure that the information ultimately reaches the community-based transmitters/receivers, erected by the electric power company, which then transmit the information back to the company by any of a variety of methods. The intense level of communication employed by this Mesh Network results in 10,000 bursts of RF radiation per day from each meter (on average) and up to 190,000 bursts of RF radiation per day (at a maximum) from each meter.[3] Because of this intense level of communication, the number of bursts of RF radiation blanketing an entire community equipped with Smart Meters can reach tens of millions to hundreds of millions of bursts per day. That does not count the bursts of radiation sent throughout the

[3] Pacific Gas and Electric Company's Response to Administrative Law Judge's October 18, 2011 Ruling Directing it to File Clarifying Radio Frequency Information, page 5. (http://emfsafetynetwork.org/wp-content/uploads/2011/11/PGERFDataOpt-outalternatives_11-1-11-3pm.pdf)

community by the community-based transmitters/receivers erected by the electric power company to communicate with the Smart Meters. I have not yet found any data on the Peak RF Power Output, or the Bursts of RF Radiation per Day, of such transmitters/receivers.

Levels of Peak RF Power Output

Four levels of Peak RF Power Output are referenced in this document:

- "Very Low" power means well below 1 milliwatt (mW) of Peak RF Power Output.
- "Low" power means 1 milliwatt (mW) of Peak RF Power Output.
- "Medium" power means 100 milliwatts (mW) of Peak RF Power Output.
- "High" power means 1000 milliwatts (mW), which is equivalent to 1 watt (W), of Peak RF Power Output.

Wired Methods of Communication

Some Smart Meters, and some AMR Meters, can be equipped to return information to the electric power company through wired communications systems. These systems employ no intentional radiators and thus do not raise health concerns associated with intentional RF radiation itself. They still employ digital electronics and switching power supplies, however; so they do still add to the level of unintentional RF radiation in the environment. Two types of wired communications systems are referenced in this document:

- The **"**Internet" can be used via wired technologies, such as coaxial cable and fiber-optic cable.
- "Telephone Landlines" can be employed that are based on copper wiring, coaxial cable, and fiber-optic cable.

Ranking Electricity Meters for Risk to Privacy and Cyber Security

Figure 2 on page 12 addresses the same Meter Categories and the same Types of Communication that are addressed in Figure 1 with regard to Risk to Health. But Figure 2 addresses the Risk to Privacy and the Risk to Cyber Security. However, for purposes of easy comparison, the overall findings for Risk to Health from Figure 1 are carried forward and placed in the Overall Risk column on the right side of on Figure 2.

Figure 2: Ranking Electricity Meters for Risk to Privacy and Cyber Security

(**RED** means risk to health. **BLUE** means risk to privacy. **GREEN** means risk to cyber security.)

Meter Category	Type of Communication			Risk to Privacy					Risk to Cyber Security			Overall Risk (5 is highest. Blank is lowest.)		
				Remote Access to Data Stream		Nature of Data			Remote Access to Meter					
	Criteria for Ranking →	*wireless*	*wired*	Number of People with Potential Remote Access	Ease of Gaining Remote Access	Timeliness	Granularity	Variety	Number of People with Potential Remote Access	Ease of Gaining Remote Access	Vulnerability of Meter to Being Harmed or to Doing Harm	Risk to Health	Risk to Privacy	Risk to Cyber Security
SMART METER Digital Advanced Metering Infrastructure (AMI)	WAN/ HAN	✓		4	5	5	5	5	4	5	5	5	5	5
	Internet cable/fiber		✓	5	2	5	5	5	5	2	5	2	4	4
	Telephone landline		✓	1	1	1	5	5	1	1	5	2	3	3
Digital Automated Meter Reading (AMR)	Bubble Up	✓		3	5	5	5	2	3	5		4	4	
	Wake Up	✓		2	5	1	1	2	2	5		3	2	
	Internet cable/fiber		✓	5	2	5	5	2	5	2		2	4	
	Telephone landline		✓	1	1	1	1	2	1	1		2	1	
Basic Digital Electronic Meter	None					1	1	1				2		
Analog Meter (plus wireless digital electronics)	Bubble Up	✓		3	5	5	5	2	3	5		4	4	
	Wake Up	✓		2	5	1	1	2	2	5		3	2	
Traditional Analog Meter	None													

Criteria for All Rankings

There are many characteristics of each electricity meter that affect the risk that it poses to health, to privacy, and to cyber security. Unfortunately, information is not publically available for many of those characteristics. The characteristics for which some information is available, and which I have selected for use here, are shown in the column headings in Figure 2.

Legitimate disagreement about the risk rankings is entirely understandable if only because there are many different configurations possible for even a single model of an electricity meter, and because individual judgment has to be exercised to produce any risk rankings. Even so, my hope is that the overall rankings presented here will be useful to identify at least:

- the type of meter that presents the highest risk
- the type of meter that presents the lowest risk
- the types of meters that fall in between, even if there is disagreement about the relative rankings of those in between.

Here are the criteria that I have used for ranking risk in each of the three risk categories:

Risk to Health

Risk to Health is higher when the RF radiation exposure produced is higher. And the RF radiation exposure is higher when the Peak RF Power Output is higher, and when the number of bursts of RF radiation per day is higher, other factors being equal.

Peak RF Power Output

Risk ↑	High Peak RF Power Output (1 watt)
	Medium Peak RF Power Output (100 milliwatts)
	Low Peak RF Power Output (1 milliwatts)
	no RF Power Output

When the Peak RF Power Output was unknown, as it was for Digital Electronics and Switching Power Supply in Figure 1 on page 6, I made an educated, but qualitative, guess, specifically “very low” and marked that entry “unknown”.

Number of Bursts of Radiation per Day

Risk ↑	High number of bursts of RF radiation per day (more than 10,000 per day)
	Medium number of bursts of RF radiation per day (There were no meters in this group, so I did not define a specific level.)
	Low number of bursts of RF radiation per day (8 per month)
	No burst of radiation, ever

When the number of bursts of radiation per day is unknown, as it was for the Home Area Network (HAN) in Figure 1 on page 6, I made an educated, but qualitative, guess of "high" and marked the entry "unknown".

Number of People Exposed to Radiation

The Risk to Health is also increased, in a societal sense, when more people are exposed to the radiation. The number of people that are exposed to the radiation is greater when the Peak RF Output Power is higher, because the size of the region exposed to the radiation increases, encompassing more people. So the Peak RF Output Power plays at least two roles in risk, increasing both the risk to each individual, and the number of individuals at risk. Thus, the heading "Number of People Exposed to Radiation" does not appear explicitly in Figure 1 on page 6.

Risk ↑	Largest number of people is reached with High Peak RF Power Output (1000 milliwatts).
	Medium number of people is reached with Medium Peak RF Power Output (100 milliwatts).
	Smallest number of people is reached with Low Peak RF Power Output (1 milliwatt).
	No people are reached with zero Peak RF Power Output.

Risk to Privacy

The criteria that affect the risk to privacy are different for different "audiences" for the data. By the *audience* I mean the people who are obtaining and exploring the data and thus invading someone's privacy. Here, I consider two different audiences:

- people *outside* of the electric power company
- the electric power company itself.

For people outside of the electric power company, the risk to privacy can be viewed as dependent on two categories of criteria:

- remote access to the data stream
- nature of the data.

But for the electric power company, which has full access to all of the data produced by its electricity meters, access is not an issue. Therefore, only the nature of the data is relevant here.

I considered what the electric power company might do with the data that it gathers, such as provide it to others outside the electric power company, which is an acknowledged public concern. That is an unknown that I could not see how to score here. But if this should occur, it would clearly be a monumental concern.

Figure 2 on page 12 can be used to assess the risk to privacy from both audiences because the criteria have been separated into the two major categories just described. However, the overall "Risk to Privacy", as reported on the right side of that figure is reflective of both categories and thus assumes that the audience is the people outside of the electric power company. Inspecting the risk rankings under "Nature of the Data" alone, the overall "Risk to Privacy" from the electric power company can be seen to be equally as high, or higher, than that from the people outside the electric power company.

Remote Access to the Data Stream

The risk to privacy increases with the number of people who can potentially gain access, and with the ease with which those people can actually gain access to that data stream. By *access* to the data stream, I mean access through the system of which the meter is a part, not access obtained by physically cutting into a wire, a cable, or a fiber.

Number of People with Potential Remote Access to the Data Stream

Risk ↑	Wired Internet data stream (both cable and fiber optic) provides the largest number of people with potential for remote access to data stream.
	Wireless data stream provides an intermediate number of people with potential for remote access to data stream.
	Wired telephone landline provides the smallest number of people with potential for remote access to data stream.
	none

When "none" applies there is no risk to privacy, no matter how the other criteria related to privacy are ranked. This case occurs for the Traditional Analog Mechanical Meter with No Wireless Communications Capability, and for the Basic Digital Electronic Meter.

Ease of Gaining Remote Access to the Data Stream

The risk to privacy also increases with the ease with which the people with potential remote access can actually gain access to the data stream.

Risk ↑	Wireless data stream is the easiest to which to gain remote access because it travels through the air.
	Wired Internet data stream (cable or fiber optic) is less easy to which to gain remote access.
	Wired telephone landline is the least easy to which to gain remote access.
	no remote data stream to access

When there is no remote data stream to access, there is no risk to privacy, no matter how the other criteria related to privacy are ranked. This case applies only for the Traditional Analog Mechanical Meter with No Wireless Communications Capability, and for the Basic Digital Electronic Meter, both of which have no wireless or wired communications capability.

Nature of the Data

The characteristics of the data affect the degree to which it is useful for invading privacy.

Timeliness

Data that are more timely are more likely to be useful for invading privacy.

Risk ↑	Timely data are more useful for invasion of privacy.
	Old data are less useful for invasion of privacy.

Granularity

Data that are more highly time resolved (more granular) are more likely to be useful for invading privacy.

Risk ↑	Highly granular (highly time-resolved) data are more useful for invasion of privacy.
	Less granular (less time-resolved) data are less useful for invasion of privacy.

Variety

Higher numbers of types of data are more likely to be useful for invading privacy.

Risk ↑	More data types are more useful for invasion of privacy.
	Fewer data types are less useful for invasion of privacy.

Risk to Cyber Security

Note that I use the phrase “cyber security” in a very limited sense in this document. The phrase refers to the security of the meter from external signals

- that can disrupt the meter itself (such as, by changing its readings or by changing its internal programming)
- that can cause the meter to do damage outside of itself (such as, by shutting down all power to the customer).

I have not considered cyber security in the sense that the meter might serve as a gateway to the network of which the meter is a part, and do damage through that network. Whether that is possible is beyond my knowledge. Certainly, if that is possible, that would be a monumental concern.

Nor have I considered cyber security in the sense that the community-based transmitters/receivers of the electric power company might serve as gateways to the network. Again, that is beyond my knowledge. If possible, that would also be a monumental concern.

Number of People with Potential Remote Access to the Meter

The risk to cyber security increases with the number of people who have potential remote access to the meter.

Risk ↑	Wired Internet data stream (both cable and fiber optic) provides the largest number of people with potential remote access to the meter.
	Wireless data stream provides an intermediate number of people with potential for remote access to the meter.
	Wired telephone landline provides the smallest number of people with potential for remote access to the meter.
	none

When “none” applies there is no risk to cyber security, no matter how the other criteria related to cyber security are ranked. This case occurs only for the Traditional Analog Mechanical Meter with No Wireless Communications Capability, and for the Basic Digital Electronic Meter.

Ease of Gaining Remote Access to the Meter

The risk to cyber security increases with the ease of gaining access to the meter remotely.

Risk ↑	Meter with wireless communications is the easiest to access remotely because all signals travel through the air.
	Meter with wired Internet communications (cable or fiber optic) is less easy to access remotely.
	Meter with wired telephone landline communications is the least easy to access remotely.
	Meter with no means of remote access.

When there is "no means" of remote access, there is no risk to cyber security, no matter how the other criteria related to cyber security are ranked. This case applies only for the Traditional Analog Mechanical Meter with No Wireless Communications Capability, and for the Basic Digital Electronic Meter, both of which have no wireless or wired communications capability.

Vulnerability of Meter to Being Harmed or to Doing Harm

The risk to cyber security increases with the vulnerability of the meter to being harmed or to doing harm.

Risk ↑	Meter has an internal shutdown switch. (That switch is always remotely controllable whenever present.)
	Meter has no internal shutdown switch.
	Meter can be accessed but has no ability to act on incoming signals.

Risk ↑	Meter has internal software that can be remotely reprogrammed.
	Meter has no internal software, or has internal software that cannot be remotely reprogrammed.
	Meter can be accessed but has no ability to act on incoming signals.

If the meter cannot act on incoming signals, it is not vulnerable in the sense meant here. Several of the meters addressed in this document appear to be invulnerable, in this sense, as shown in Figure 2 on page 12.

Limitations to this Analysis

There are many limitations to this analysis:

- The variety of electricity meters available is so great that not all of them could be addressed here.
    - That variety is increased by the availability of hardware options and software programmability for some of the meters.
    - Some of the hardware options can be implemented not only by the manufacturers of the meters, but also by the electric power companies, both before installation and after installation.
    - Some of the software programmable capabilities can be exercised not only before installation but also after installation, and even *remotely* after installation and thus invisibly to the customer.
- The risk presented by a given meter is highly dependent on the options included in it. So the generalizations made here for a given category of meters may apply to a greater or a lesser degree depending on those options.
- New meters are being created all the time.
- It is impossible to obtain all of the information pertinent to assessing the risk of a given meter to health, privacy, and cyber security, for several reasons:
    - Some of the information needed is regarded as confidential or proprietary
        - by the manufacturers of the meters
        - by the testing laboratories that prove the compliance of the meters with the regulations of the Federal Communications Commission
        - by the electric power companies that buy and install the meters for their customers.
    - Some manufacturers and electric power companies decline to provide information about the meters, even if that information is not formally considered confidential or proprietary. No reason is usually given.
    - Some of the information needed may never have been generated.

- Even for information that exists, there may be no legal requirement for that information to be revealed to the public, short of a court order. Such a court order has been employed in at least one instance, and provided vital information about Wireless Smart Meters that it had not been possible to locate previously.[4]

Closing

In spite of the limitations of this analysis, I hope that this document gets close enough to capturing the principal distinctions among the many types of meters addressed here to provide some useful perspective on their relative risk. Perhaps this document will motivate those who know more about the meters to develop their own ranking.

[4] Pacific Gas and Electric Company's Response to Administrative Law Judge's October 18, 2011 Ruling Directing it to File Clarifying Radio Frequency Information, page 5. (http://emfsafetynetwork.org/wp-content/uploads/2011/11/PGERFDataOpt-outalternatives_11-1-11-3pm.pdf)