

E-00000C-11-0328

ORIGINAL

OPEN MEETING AGENDA ITEM  
ARIZONA CORPORATION COMMIS



UTILITY COMPLAINT FORM

Investigator: Scott Friedson

Phone:

Fax:

Priority: Respond Within Five Days

Opinion No. 2013 - 108626

Date: 2/20/2013

Complaint Description: 01H Billing - Smart Meter  
N/A Not Applicable

Complaint By: First: Nancy Last: Baer

Account Name: Nancy Baer

Home: (000) 000-0000

Street: Unknown

Work:

City: Unknown

CBR:

State: AZ Zip: 99999

is:

RECEIVED  
2013 FEB 21 A 10:55  
AZ CORP COMMISSION  
DOCKET CONTROL

Utility Company: Miscellaneous Electric

Division: Electric

Contact Name: Unknown

Contact Phone: (000) 000-0000

Nature of Complaint:

2/20/13

Subject: FW: AZ CC DOCKET E00000C-11-0328 - DAVID CHALK, CYBERSECURITY EXPERT RESPONSE TO DRAFT OPT-OUT AND PRIVACY GUIDELINES DATED 10/23/12

Importance: High

"The utility company cannot guarantee with certainty that the data is safe and it will force you to agree to allow them to share it under certain circumstances." David Chalk, D. Tech.

Dear Public Officials:

I submit the attached response to the Arizona Corporation Commission Utility Division's draft opt-out and privacy guidelines of 10/23/12 contained by a telephone interview that I and my colleague, Monnie Ramsell conducted with Dr. David Chalk, Cybersecurity Expert. For those who are unfamiliar with Dr. Chalk I am providing a synopsis of his professional experience qualifying him as an expert to comment on the proposed guidelines below.

Nancy Baer, APS Consumer

David Ian Chalk, D.Tech  
www.davidchalkinc.com  
www.decision-zone.com

Founder, Chalk Media (sold to Research in Motion), 1997-2007  
Founder, Doppler Computer Superstores, 1985-1997

Holder of U.S. patent US7908160 (<http://www.google.com/patents/US7908160>) "Vulcan Anomaly Detection" for a safe power grid. The patent is specific to full protection of the Power Grid with Certainty. Col. Robert Banks, US Cyber Command Deputy Director, US Army, supports this technology which has been tested and proven.

Arizona Corporation Commission  
DOCKETED

FEB 21 2013

DOCKETED BY *JM*

# ARIZONA CORPORATION COMMISSION

## UTILITY COMPLAINT FORM

---

Chalk also developed the first video streaming and content engine for Yahoo! in 1999. He has consulted industry leaders including Bill Gates, Martha Stewart and Charles Wong.

Chalk has been awarded for his work with companies including Verizon USA, Sony, Samsung, RIM, Microsoft, Business Objects, and many others. In early 2000, Chalk received a Freddie Award for Best International Educational Documentary: "An insight into life with Dyslexia & learning disabilities."

In the late 2000s, Chalk brought Decision-Zone software to market, which allows for real-time detection of business process anomalies. The technology is capable of 100% fraud and system security protection in sectors such as banking, insurance, healthcare, the military and Cyber Defense.

---

### Attachment Information:

"The utility company cannot guarantee with certainty that the data is safe and it will force you to agree to allow them to share it under certain circumstances."

Dr. David Ian Chalk, .d.Tech  
www.davidchalkinc.com  
www.decision-zone.com

Founder, Chalk Media (sold to Research in Motion), 1997-2007  
Founder, Doppler Computer Superstores, 1985-1997  
Holder of U.S. patent US7908160 ( <http://www.google.com/patents/US7908160>) for a safe power grid, "Vulcan Anomaly Detection. 11 The patent is specific to full protection of the Power Grid with Certainty. Col. Robert Banks, US Cyber Command Deputy Director, US Army, supports this technology which has been tested and proven.

Chalk also developed the first video streaming and content engine for Yahoo! in 1999. He has consulted industry leaders including Bill Gates, Martha Stewart and Charles Wong.

Chalk has been awarded for his work with companies including Verizon USA 1 Sony, Samsung1 RIM, Microsoft, Business Objects, and many others. In early 2000, Chalk received a Freddie Award for Best International Educational Documentary: "An insight into life with Dyslexia & learning disabilities."

In the late 2000s, Chalk brought Decision-Zone software to market, which allows for real-time detection of business process anomalies. The technology is capable of 100% fraud and system security protection in sectors such as banking, insurance, healthcare, the military and Cyber Defense.

The following is a transcript of David Chalk's responses to the Arizona State Corporation's Utility Division draft opt-out guidelines.

#1 Unless authorized by the customer or the Arizona Corporation Commission, electric usage measurement will not be specific to any particular appliance or electrical device. Meters with the capability to only measure a single electrical device or a group of such devices will be permitted under this guideline.

DC The utility company's computer system is not designed to do that, it does not have that capacity. Looking at the inherent ability of electric signals, it is clear to see why it is not possible. Every time a device is turned on, or electricity is used, it puts a unique signal on the line. Consider electricity as a very complicated pattern, not just as a flow of electrons. From a bird's eye view at a crowd of people below, you would see that if somebody ran through the crowd, it would cause a disruption to the flow of the crowd. If two or three people started running into the crowd, people would start moving aside. The discernible patterns as the people in the crowd move are comparable to electricity flowing; when a single

# ARIZONA CORPORATION COMMISSION

## UTILITY COMPLAINT FORM

---

device that is turned on is recognizable and as it draws more or less power, or when it's turned on or off, how that particular device is being used you can track. The utility is claiming that these devices are not used to measure individual devices. The point is that if the data is looked at by applications that know how to interpret it, it's very clear and easy to see exactly what is going on.

#2 Unless authorized by the customer, the utility will not share customer-specific data except with entities under contract with the utility and bound to comparable confidentiality provisions as would apply to the utility itself. However, such authorization is not required if the data is requested by law enforcement or other public agencies, including the Commission or its staff, or is used in conjunction with legitimate collection activities, or to provide safe and reliable service to the customer. Customer-specific data will never be sold without customer approval. Usage data unaccompanied by any other information that would associate the usage data with a specific customer (e.g., customer name, service address, telephone number, SS# or EIN, etc.) is not considered "customer-specific data for the purposes of this guideline.

DC The utility company is admitting that it has complex confidential information and that regardless of whether they are going to do something with it, or not, someone acting as a hacker can. How is this information protected? So that is the first problem with the utility company's statement. Indeed, this is borne out recently by the largest data theft in U.S. history that occurred at the end of October. Seventy-five percent of the State of South Carolina's citizens' records in its Department of Revenue were hacked by rogue hackers, not a nation/state, from the Soviet Union. Citizens' personal information along with their tax returns, etc. were stolen (<http://rt.com/usa/news/hacker-south-carolina-soda1-security-credit-400/>). The State of South Carolina has had to spend billions of dollars purchasing individual insurance policies to cover all of these citizens for the rest of their lives. If hackers could break into the U.S. Internal Revenue Service and take that information and have those people vulnerable for life, do you think a power company, once that information is taken is ever even going to admit to it, let alone put a life long insurance policy on you?

So who exactly who bears liability when the utility says it can share your information with the commissioner, or his staff, or with legitimate collection activities? What happens when the mail person, who may be considered "staff" within the commissioner's office loses an envelope, as often occurs, and has no idea where it was misplaced, who is liable in that case?

What consumers need to realize is once the information is electronic it may not be possible to know that the mail person lost an envelope. You may not even know it was taken and what the power company will do. As I said when you use certain online services, such as FB and iTunes you must agree to accept that they're not responsible for the loss of the information, whereas the government takes responsibility for such losses. The utility company cannot guarantee with certainty that the data is safe and it will force you to agree to allow them to share it under certain circumstances. Now the only concern that I believe should be fought on this is, as you say, "agreed", but at the same time, consumers must receive written confirmation that their information is secure in the meantime.

Secondly, the consumer needs to be aware that the utility company will probably ask its consumers to "agree" to certain terms electronically by an Unlimited License Agreement (ULA) to allow the user to perform various functions, much like Facebook or iTunes operate. If you read through these hundreds of pages they contain specifics about how they will, and can use, your information. If you don't agree to certain things, you will not be able to use these services.

As it adds more services, as is likely if it is to become a "big data" center the consumer likely will have to agree electronically to accept a service they formerly refused in order to get the "new" feature.

#3 Customer specific data wirelessly transmitted between meters and the utility must be encrypted and/or password protected. The utility will use recognized industry security practices and controls and will continue to evaluate emerging technologies and standards in order to update its security practices, as appropriate, to protect customer specific data.

DC The utility company is admitting that it is continuing to upgrade the technology as new technology comes along. The technology as designed, isn't final and complete. This guideline is a coy move giving the appearance to the un-indoctrinated that its "smart" meters are safe. But, if I said to you something was

# ARIZONA CORPORATION COMMISSION

## UTILITY COMPLAINT FORM

---

not poison and "I want you to drink it," and then I said to you, "by the way that we're continuing to test it." Well that doesn't mean that it is not poison, but rather we think it is probably not poison. It's not poisoned by the tests that we can do, so maybe it's going to maybe kill you 17 years from now, but there's not a test currently in existence that can prove it that far into the future.

Secondly, any encryption can be de-encrypted with the de-encryption tool being used at the other end. So, let's just understand that digital information is digital information and I can just steal the decrypting key and decrypt it. On top of that, why (acting as a hacker) don't I just get the data before its encrypted? I don't care if I get it over the wire. Data is like water. Water is water wherever it is. I can get it; before it goes into the tap, after it comes out of the tap, or while it's flowing in the sewer pipe. I can get it wherever I want. So again, this is a ploy the utility company uses on everyone to have the uninformed believe there's some magical thing about from your house to the neighbor's next door, even if it's encrypted, I'll just take it from your house, or the neighbor's, or the utility's warehouse.

As a hacker, I'm looking for collective data. I'm looking for patterns. I'm looking for usage. I'm looking for how many air conditioners go on in a community, or how often do the lights go out at night, or how often do they turn their burglar alarm on. I can tell all those things collectively, so I may not care about you individually I'm looking for millions of pieces of data to find out what I want.

However, if you are a "person of interest" a hacker can get your information. At the same time, whether it is encrypted at your device or not, it is going to be unencrypted at some point so a hacker may just wait until it's put into the utility's data base.

Everything the utilities claim is always about some minute point regarding a component of how the data is being handled; where it's going/ or where it's going to be. A hacker can get it from anywhere.

Computer systems and their protection are all designed one way; that is, they collect data. Now data is about something that has already happened. There is a void vacuum. If nothing is happening, there is no data.

#4 Data from each meter must use unique identifier(s) associated with the customer's service to ensure that each customer is billed only for his/her own usage.

What difference does it make to have a unique identifier? None.

#5 The utility will not control or shut off individual appliances without customer consent or unless authorized by an approved Arizona Corporation Commission tariff or program.

First, the utility company may not shut off your power but a hacker, or some rogue nation/state or will. Secondly, of the many issues involved with this matter, two of the most major are; whether or not the low frequency radiation coming from the devices effects humans and, the matter related to the harvesting of the data 1 which contains my personal information is not being kept secured.

#6 The utility may shut off electric service per Arizona Corporation Commission rules or other Commission-approved procedures. The utility will abide by current regulations or other Commission-approved procedures with respect to shut-off of service and curtailment in power emergencies.

DC I think that as the utility is saying that current procedures apply because today if you don't pay your bill, or if there is any incident, they will shut the power off that's par for the course.

#7 The utility will only use equipment that limits data transmission, so as to keep radio frequency exposure within the limits established by the Federal Communications Commission.

I think you can look online and see that those devices, once they are in the mesh, can be sending out billions of transmissions. Regardless of that, there is the determination of what level of radiation is dangerous to humans. A recent study sited that that low levels of radiation resulted in damage to cytokine production which may result in cancer (Iraj Salehi, et al., Electromagnetic Biology and Medicine/ Early Online: 1-8, 2012,

**ARIZONA CORPORATION COMMISSION**  
**UTILITY COMPLAINT FORM**

---

Copyright © Informa Healthcare USA, Inc., ISSN: 1536-8378 print/1536-8386 online DOI: 10.3109/15368378.2012.692343.

Per Curtis Bennett, Chief Science Officer/ Interprovincial Journeyman Electrician (Red Seal), Building Construction Engineering Technologist, "The FCC declaring safety is only addressing the meter as an end use device, the rest of the wireless circuit; routers, relays, etc.. Were not accounted for or included in the FCC's calculations" (Expert Witness testimony submitted to Brady, TX ).

#8 The utility shall allow customers to request, and have installed, meters that do not transmit data wireless/y. For those customers that request to have a meter that is not capable of transmitting data wirelessly and where the utility is using only meters that transmit data wirelessly, the utility may propose a tariff, for Arizona Corporation Commission's consideration, that would recover appropriate costs from such a customer.

This particular "guideline" makes it very clear that the benefit accruing to the utility companies derives from the harvesting of the information. Otherwise, they would not be so anxious to get these meters installed. The proof is seen in Silicon Valley now that where one of the highest funded and most rapidly advancing markets in technology is technology applications to; monitor, harvest, investigate and report on mass data which is called "big data" data collected from utility data centers. This is even echoed at the U.S. Federal level with the national data center in Nevada. Now, if those technologies are getting capitalized faster than anything else, I think then we can easily draw the conclusion that there is a lot of money in collecting this data. This is evidenced by the utility company/s rush to replace analog meters with digital ones. I have observed that in most cases, utility companies do not define policy regarding 'opt-out' until after the meters have been installed under conditions unknown to the consumer, or when the consumer signed up for 'time of use' billing.

That's a strong arm method to get you to follow whatever they want. If the utility company switches its devices to anything that's technologically based, there's a much higher cost of operating it than for analog. When I was a child, I grew up in a house that's already 30 years old and the meter I believe is still on that, making the meter probably 50 years old. Whether or not it gets replaced, it will continue to run. In the technology world, 'smart' meter manufacturers claim 1 in many cases, that those meters are specified to last 8 to 12 years. More than likely, these meters will only last 2-3 years with an unknown replacement cost depending on where they are located that could be collectively cost hundreds of millions, if not billions of dollars.

Naturally, it will lower the companies' labor and truck maintenance costs to eliminate meter readers having to go and inspect and turn on and off meters. However, the consumer is put at even greater risk, in addition to identity theft, should there be a mechanical problem with the meter itself that causes a fire. Only a human being can give a knowledgeable real time inspection of anything.

So the utility company will minimize that issue because it's in its best interest to maintain that they don't need people, because it is the very same people as those that no longer witness the data in the filing cabinet that is secure and would know if the files had disappeared.

Here's the thing you need to know. Microsoft who makes 'smart' meters admits that "There is no way to guarantee complete security on a wireless network."

<http://windows.microsoft.com/en-US/windows-vista/How-do-I-know-if-a-wireless-network-is-secure>.

\*End of Complaint\*

**Utilities' Response:**

**Investigator's Comments and Disposition:**

Recorded for the record and filed in docket number E-00000C-11-0328. FILE CLOSED.

\*End of Comments\*

**Date Completed: 2/21/2013**

ARIZONA CORPORATION COMMISSION  
UTILITY COMPLAINT FORM

---

Opinion No. 2013 - 108626

---