Hackers see "sheeple" sheared by Google wireless data grab

July 30 2012, by Glenn Chapman

Long before Google online mapping service cars snatched data from private wireless hotspots there was the Wall of Sheep.

The Wall, created by Aires Security, has long been a mainstay of the infamous Def Con gathering of hackers that ended Sunday in Las Vegas.

Designed as a "security awareness tool" and refined over the years, the Wall captures data sent wirelessly by smartphones, laptops or other gadgets and then finds information unguarded by encryption or tough passwords.

Wall builders have long branded folks careless about what they send wirelessly as "sheeple" vulnerable to wolves who can eavesdrop on transmissions as easily as one can overhear a chat in a coffee shop.

Those behind the Wall see what Google did by sucking up unprotected wireless data with Street View vehicles as perhaps unethical but perfectly legal.

"If you overhear a conversation in a public place, a Starbucks for example, you are not doing anything illegal," Aires chief Brian Markus said as private data of "sheeple" was projected on a wall behind him.

"For wireless, if you are monitoring it passively and you don't have to break into anything that should be legal."

The Wall team's T-shirts this year were emblazoned with "Encrypt or you will regret it in the end."

The subject of whether the Wall, and by extension what Google did with Street View, was criminal was the focus of a Def Con session where hackers backed the idea that unprotected data was fair game.

"Tech people think sniffing is fine; people who understand privacy think it's terrible," University of Pennsylvania distributed labs director Matt Blaze said during the session, referring to capturing wireless data.

"If you understand both, your head explodes."

Attorney Kevin Bankston of the Center for Democracy and Technology played devil's advocate in the discussion, itemizing points of US law that work against Google's in the Street View controversy.

"Whatever you think of this issue it is dead clear that the law is a mess," Bankston said.

Bankston said a key point was that while overhearing conversations isn't crimes, capturing wireless communications is unless the communication "is readily available to the general public."

Markus considered wireless transmissions to be just that, since gear to "sniff" the airwaves is easily available.

"With the Wall of Sheep, we are kind of implying that people who can't figure out how to set up their routers deserve about the same level of protection as sheep," Blaze said.

"Don't punish people for not being able to figure out how to turn on the crypto."

Markus was quick to agree that the technically un-savvy don't deserve to have their privacy trampled.

"We are concerned about the everyday user, which is why we are trying to get the message out there," he said of the purpose behind the Wall.

"Legislation is not going to stop the problem," he continued. "The answer is to push companies to fix it."

WiFi gear that doesn't encrypt data by default is a dying breed, according to Blaze.

Bankston was worried that US justice officials would take advantage of the mood in Washington to expand how much wireless data they could grab from people.

"How about a little sniffer on every cop's belt, or in every cruiser?" he asked rhetorically.

"The Department of Justice hasn't said how they read the law right now, which is notable and worrisome."

The Federal Communications Commission (FCC) in April dropped its Street View investigation, saying it could not accuse Google of breaking US law but fining the company $25,000 for what it saw as slow cooperation.

The FCC began the investigation in late 2010 after Google announced that Street View cars taking photographs of cities in more than 30 countries had inadvertently gathered data sent over unsecured Wi-Fi systems.

Information sucked up by passing Street View cars included passwords,

emails, and other data that was being transmitted wirelessly over unprotected routers, according to the FCC.

Google has since stopped the collection of Wi-Fi data, used to provide location-based services such as driving directions in Google Maps and other products, by Street View cars.

Street View, which was launched in 2006, lets users view panoramic street scenes on Google Maps and take a virtual "walk" through cities such as New York, Paris or Hong Kong.