How an internet mapping glitch turned a random Kansas farm into a digital hell

Kashmir Hill

4/10/16 10:00AM • Filed to: REAL FUTURE

Elena Scotti/FUSION

An hour's drive from Wichita, Kansas, in a little town called Potwin, there is a 360-acre piece of land with a very big problem.

The plot has been owned by the Vogelman family for more than a hundred years, though the current owner, Joyce Taylor née Vogelman, 82, now rents it out. The acreage is quiet and remote: a farm, a pasture, an old orchard, two barns, some hog shacks and a two-story house. It's the kind of place you move to if you want to get away from it all. The nearest neighbor is a mile away, and the closest big town has just 13,000 people. It is real, rural America; in fact, it's a two-hour drive from the exact geographical center of the United States.

But instead of being a place of respite, the people who live on Joyce Taylor's land find themselves in a technological horror story.

For the last decade, Taylor and her renters have been visited by all kinds of mysterious trouble. They've been accused of being identity thieves, spammers, scammers and fraudsters. They've gotten visited by FBI agents, federal marshals, IRS collectors, ambulances searching for suicidal veterans, and police officers searching for runaway children. They've found people scrounging around in their barn. The renters have been doxxed, their names and addresses posted on the internet by vigilantes. Once, someone left a broken toilet in the driveway as a strange, indefinite threat.

All in all, the residents of the Taylor property have been treated like criminals for a decade. And until I called them this week, they had no idea why.

📡📡📡

To understand what happened to the Taylor farm, you have to know a little bit about how digital cartography works in the modern era—in particular, a form of location service known as "IP mapping."

IP refers to an Internet Protocol address, which is a unique identifier assigned to a computer or a computer network. IP addresses play an essential role in computers talking to each other, and every internet-connected device needs one. The device you're using to read this article has an IP address, and when you visited this site, our servers wrote it down. So we now have a record that someone using that particular IP address read this story in our server logs. Sometimes, through some sophisticated

sleuthing, you can find out more information about a specific IP address—for example, whether it's been associated with a malicious device, or where in the world it's located.

The trouble for the Taylor farm started in 2002, when a Massachusetts-based digital mapping company called MaxMind decided it wanted to provide "IP intelligence" to companies who wanted to know the geographic location of a computer to, for example, show the person using it relevant ads or to send the person a warning letter if they were pirating music or movies.

There are lots of different ways a company like MaxMind can try to figure out where an IP address is located. It can "war-drive," sending cars around the U.S. looking for open wifi networks, getting those networks' IP addresses, and recording their physical locations. It can gather information via apps on smartphones that note the GPS coordinates of the phone when it takes on a new IP address. It can look at which company owns an IP address, and then make an assumption that the IP address is linked to that company's office.

But IP mapping isn't an exact science. At its most precise, an IP address can be mapped to a house. (You can try to map your own IP address here.) At its least precise, it can be mapped only to a country. In order to deal with that imprecision, MaxMind decided to set default locations at the city, state and country level for when it knows only roughly where the IP address lives. If it knows only that an IP address is somewhere in the U.S., and can't figure out anything more about where it is, it will point to the center of the country.

Read more

As any geography nerd knows, the precise center of the United States is in northern Kansas, near the Nebraska border. Technically, the latitudinal and longitudinal coordinates of the center spot are 39°50′N 98°35′W. In digital maps, that

number is an ugly one: 39.8333333,-98.585522. So back in 2002, when MaxMind was first choosing the default point on its digital map for the center of the U.S., it decided to clean up the measurements and go with a simpler, nearby latitude and longitude: 38°N 97°W or 38.0000,-97.0000.

As a result, for the last 14 years, every time MaxMind's database has been queried about the location of an IP address in the United States it can't identify, it has spit out the default location of a spot two hours away from the geographic center of the country. This happens a lot: 5,000 companies rely on MaxMind's IP mapping information, and in all, there are now over *600 million* IP addresses associated with that default coordinate. If any of those IP addresses are used by a scammer, or a computer thief, or a suicidal person contacting a help line, MaxMind's database places them at the same spot: 38.0000,-97.0000.

Which happens to be in the front yard of Joyce Taylor's house.

A gift from one of the house's many random visitors

"The first call I got was from Connecticut," Taylor told me by phone this week. "It was a man who was furious because his business internet was overwhelmed with emails. His customers couldn't use their email. He said it was the fault of the address at the farm. That's when I became aware that something was going on."

This was back in 2011. Taylor, who grew up on the farm and remembers the day when she was 15 when the house first got an indoor bathroom, has a Gateway computer but doesn't use the internet often. "I use it to write letters and Sunday school lessons," she says. When I first called her, she refused to talk to me because she's had so many crazy callers over the years. "My parents had a golden reputation. My family has always been beloved in this community," she told me by phone later. "We've never had enemies."

But over the next several months, the calls and visits intensified. When law enforcement agents asked companies like Google and Facebook for the IP addresses used by suspected criminals and then mapped them using tools like this that relied on the MaxMind database, it pointed at the Taylor house. Amateur sleuths who spotted IP addresses used by visitors to their websites or on message forums were so convinced that the Taylor house was the source of their various problems that they created reports about it on Facebook, YouTube, Reddit, the Ripoff Report and Google Plus. (Even today, if you Google the house's address, it returns a series of websites detailing nefarious activities.)

The harassment continued to the point where the local sheriff had to intervene. He placed a sign at the end of the driveway warning people to stay away from the house and to call him with questions.

"That poor woman has been harassed for years," Butler County Sheriff Kelly Herzet told me by phone. Herzet said that his department's job has become to protect the Taylor house from other law enforcement agencies. "Our deputies have been told this is an ongoing issue and the people who live there are nice, non-suicidal people."

Last year, I discovered a young couple in Atlanta that suffered from a similar, but less severe, issue: Since the couple moved into their home a year ago, dozens of strangers have visited looking for lost and stolen smartphones. The visitors are led there by Find-My-Phone apps that say the phones are located inside the house. (They aren't.) While helping the couple try to figure out their mystery, I teamed up with the podcast Reply All and a security researcher named Dave Maynor. When Maynor visited the house to investigate, he discovered that it was one of the only houses in the neighborhood with a router and wifi. The couple lived in a digital desert, and because of the way some location mapping works, looking for a permanent network in the area to act as an anchor, lots of IP addresses were getting attached to the house.

After I published that story, I began wondering if there were other homes in the country like it. I asked Maynor if there was a way to find out and he said he could build a program that would crawl through a public Maxmind database of mapped IP addresses to see if there were physical locations that appeared repeatedly. Within a couple of days, he had sent me a spreadsheet with thousands of home addresses along with the number of IP addresses attached to them. The Taylor home was at the very top of the list; the 600 million IP addresses attached to the home were an order of magnitude higher than at any other location. (The Atlanta home was number 865 on the list.)

Earlier this week, I reached Thomas Mather, a co-founder of MaxMind, via email. I told him Joyce Taylor's story, and how I'd discovered MaxMind's involvement in the IP mapping part of it. I asked him if he knew anything about the default coordinates that were placing unidentified IP addresses on the Taylor's property.

Mather told me that "the default location in Kansas was chosen over ten years ago when the company was started."

He continued: "At that time, we picked a latitude and longitude that was in the center of the country, and it didn’t occur to us that people would use the database to attempt to locate people down to a household level. We have always advertised the database as

determining the location down to a city or zip code level. To my knowledge, we have never claimed that our database could be used to locate a household."

But people *do* use it that way. Five thousand companies draw information from MaxMind's database. And most casual internet users don't know anything about IP mapping defaults—they just know that when a website tells them that their scammer lives in Potwin, Kansas, they get in the car and go.

"A lot of apps use this data without warning people it's not scientifically accurate," said security researcher Maynor. "How do you educate people that the thing popping up on their screen as the location of an IP address isn't reliable?"

Read more

Mather, the MaxMind co-founder, told me that he hadn't realized until I emailed him that his IP mapping had caused problems for Joyce Taylor and her tenants. But he sounded sympathetic.

"Until you reached out to us, we were unaware that there were issues with how we selected these lat/lons," said Mather by email. "We do take this issue seriously and are working to resolve it as quickly as possible."

📡📡📡

The Kansas house is not the only house to have problems as a result of being a default location in the MaxMind database. I also spoke with a man in Virginia who has experienced similar problems for years.

Tony Pav lives in a house at the end of a cul-de-sac in Ashburn, Virginia. Among other things, Ashburn is home to a number of large data centers—the giant buildings that companies like Google and Facebook use to store their huge clusters of servers. As

a result of all of these data centers, there are a gigantic number of IP addresses associated with Ashburn—more than 17 million in all.

And due to the way MaxMind selected its default locations, all 17 million of these IP addresses appeared to be located in Pav's home.

Pav told me he first started experiencing problems four years ago. In 2012, he came home late one night to find the police about to break down his door. They said they were looking for a stolen government laptop with personal information on it. He let them in to search; it wasn't there, even though its IP address was pointing right at his house.

"They tore up my house looking for it, and found nothing," he said.

The consequences of a mapping glitch: a search warrant presented to Pav in 2012

He's gotten angry phone calls and Facebook messages from strangers who've been wronged by someone online. When they track the IP addresses associated with their assailants, they point to his house, so they assume its occupants are responsible.

"Other than the humiliation of having my house raided by law enforcement, I have genuine concerns for my safety should someone come directly to my house because of

this faulty data," Pav told me by phone. "It's like having a target pointed directly at you. I feel like I'm sitting on a time bomb."

Pav has plans to retire in three years, and thought he wouldn't be able to sell his home when he had to disclose the problems it had. Like the people at the Kansas house, Pav had no idea why this was happening. They'd never heard of MaxMind before. The company is part of the technological infrastructure of the internet that they didn't know existed, and certainly didn't realize had chosen their homes as key points in its database.

"I felt helpless," said Pav.

The physical mapping of computer addresses is one of the many aspects of the internet infrastructure that is almost completely unregulated. It is a task performed by private companies, and not just MaxMind. No one is officially in charge, and so there was no obvious party that Tony Pav or Joyce Taylor could go to in order to find out why this was happening, or get it fixed.

There are lots more of these phantom IP houses. When Dave Maynor sent me that list of thousands of locations in the MaxMind database that have aberrantly high number of IP addresses associated with them, my colleague Kristen Brown and I called dozens of them. Many remain blissfully unaware that they're living in an IP flood zone; they'd never had strangers show up on their doorstep. Apparently, the IP addresses attached to their homes haven't yet been used for anything nefarious. Yet.

One important lesson of my sleuthing is that IP addresses, which get used as digital evidence in criminal trials and to secure search warrants, are not always reliable. Like Social Security numbers, they were a numerical system built for one purpose that are now used for something completely different. Social Security numbers were designed to keep track of a person's earnings over their lifetime, but are now the security token used to lock down their entire identity. IP addresses were meant to allow computers to talk to each other, but have been repurposed to reveal details about the person behind

that computer. The words "security" and "address" in their titles promise more than they can deliver.

Now that I've made MaxMind aware of the consequences of the default locations it's chosen, Mather says they're going to change them. They are picking new default locations for the U.S. and Ashburn, Virginia that are in the middle of bodies of water, rather than people's homes.

Read more

I asked Mather how soon all of the companies that use its IP mapping database will update the information in their own databases.

"I'd say the typical customer updates the data every week, but that can vary," said Mather. "Some customers only update every few months."

MaxMind will refresh its database next Tuesday. And the Taylor farm will, hopefully, be a quiet place again sometime soon.