euclid

March 28, 2013

The Honorable Al Franken
United States Senate
309 Hart Senate Office Building
Washington, DC 20510

Dear Senator Franken,

I write to answer the questions you raised in your letter dated March 13, 2013. Like you, I believe in the importance of protecting consumer privacy both online and in the real world, and I appreciate the opportunity to explain how Euclid is addressing the privacy concerns that we both champion.

Euclid was founded through the passion of my grandfather, John Smith, who was one of the first developers of the modern-day shopping center. As a developer, his primary goal was to improve the shopping experience: Happy shoppers buy more. Dissatisfied shoppers leave quickly. However, during his lifetime, he did not have robust data to guide his choices. My grandfather's decisions about design, store mix, and traffic flow were guided only by his experience and intuition. The most sophisticated analytical tool he possessed was a turnstile with a counter.

With the advent of the Internet, there has been an explosion in online shopping. The analytical tools available to online retailers have enabled them to rapidly increase the effectiveness of their marketing, distribution, and sales. Using these insights, online stores are able to offer a more convenient and relevant shopping experience and now account for 5.2 percent of total U.S. retail sales.

About three years ago, we founded Euclid to bring the advantages of the online customer experience to brick-and-mortar retailers. We believe these establishments still play a vital role in our communities, accounting for 9.3 percent of the nation's workforce and contributing $848.5 billion dollars to the recovering American economy. As just one example, last year alone the Twin Cities' Mall of America employed 11,000 workers and contributed nearly $2 billion to Minnesota's economy.

Conscious of the evolving privacy debate in the world of online retail, we set about to design a product that, from the outset, would safeguard consumer privacy and address potential concerns. This process is commonly known as Privacy by Design. We consulted respected organizations, academics, and advocates in the privacy community in our efforts to design a product that both provides valuable insights and protects consumer privacy. Most importantly, we made sure that our system never receives information such as a consumer's name, address, phone number, or email.

Here is how Euclid's sensors work. Every smart device equipped with Wi-Fi (including mobile phones, laptops, tablets, and e-readers) has a unique identifier known as a MAC address. These devices regularly send out signals ("pings") that contain their MAC address to find Wi-Fi hotspots, such as those commonly found at coffee shops, airports, and in public spaces. When a shopper carrying a smart device walks by a retail store, the Euclid sensor at the store recognizes the broadcasted ping, scrambles the MAC address into what is known as a hash, discards the MAC address data, and sends the hashed value to Euclid's servers. In addition to the anonymous hash, the sensor also transmits basic device data received by our sensors: manufacturer code (Apple, Samsung, etc.), signal strength, and, if the device is currently connected to a specific Wi-Fi network, and the name of that Wi-Fi network.

We use this anonymous data to derive aggregated insights about in-store traffic that are shared with the retailer. The retailer can use these metrics to better understand how staffing, merchandising, and window display changes might affect the number of visitors who enter their store and stay long enough to complete a purchase. A retailer would receive information like this: “Today 300 potential customers walked by your storefront and 150 entered. Of the 150, 15 percent stayed for less than 5 minutes, 55 percent stayed for 5-15 minutes and 30 percent stayed for longer than 15 minutes.” Euclid improves the customer experience by helping retailers pinpoint specific ways to reduce wait times, extend business hours, and improve staffing levels. Using Euclid’s tools, retailers can operate more efficiently, stay competitive, and serve their customers better.

Your questions have led us to closely examine our product and work. Having an innovative product that helps both consumers and retailers is not enough. We support your efforts and we therefore renew our dedication to bringing value while striving to protect consumers and their right to privacy. To that end, Euclid reaffirms its commitments that protect consumer privacy:

- Our sensors receive only the following basic data: MAC address, manufacturer code (Apple, Samsung, etc.), signal strength, and, if the device is currently connected to a specific Wi-Fi network, the name of that Wi-Fi network.
- We cannot and never will receive any information relating to names, addresses, phone numbers, emails, etc.
- We never share information on individual devices.
- We never link data to specific individuals.
- We never share information between our clients.
- We provide a permanent opt-out process for any customer who wishes to do so. Our in-store notices direct customers to our website, which features a simple process by which customers can permanently opt out and delete data from our service.

In addition, Euclid makes the following new commitments to further protect consumer privacy:

- We will include posted customer signage as a stipulation in our contracts with all retailers going forward.
- We will institute a new and comprehensive education program about the opt-out process that we will require all retailers to undergo.
- We will strengthen our privacy policy to prohibit the sale, rental, or disclosure of any of Euclid’s data to data brokers.
- We will create a formal policy outlining our requirements for a warrant or court order to comply with any request for data, which we will rely on in case we should ever receive such a request.

We sincerely appreciate your efforts in this area and have attached our answers to your questions. We see this as just the beginning of an important dialogue and look forward to partnering with you in support of consumer privacy.

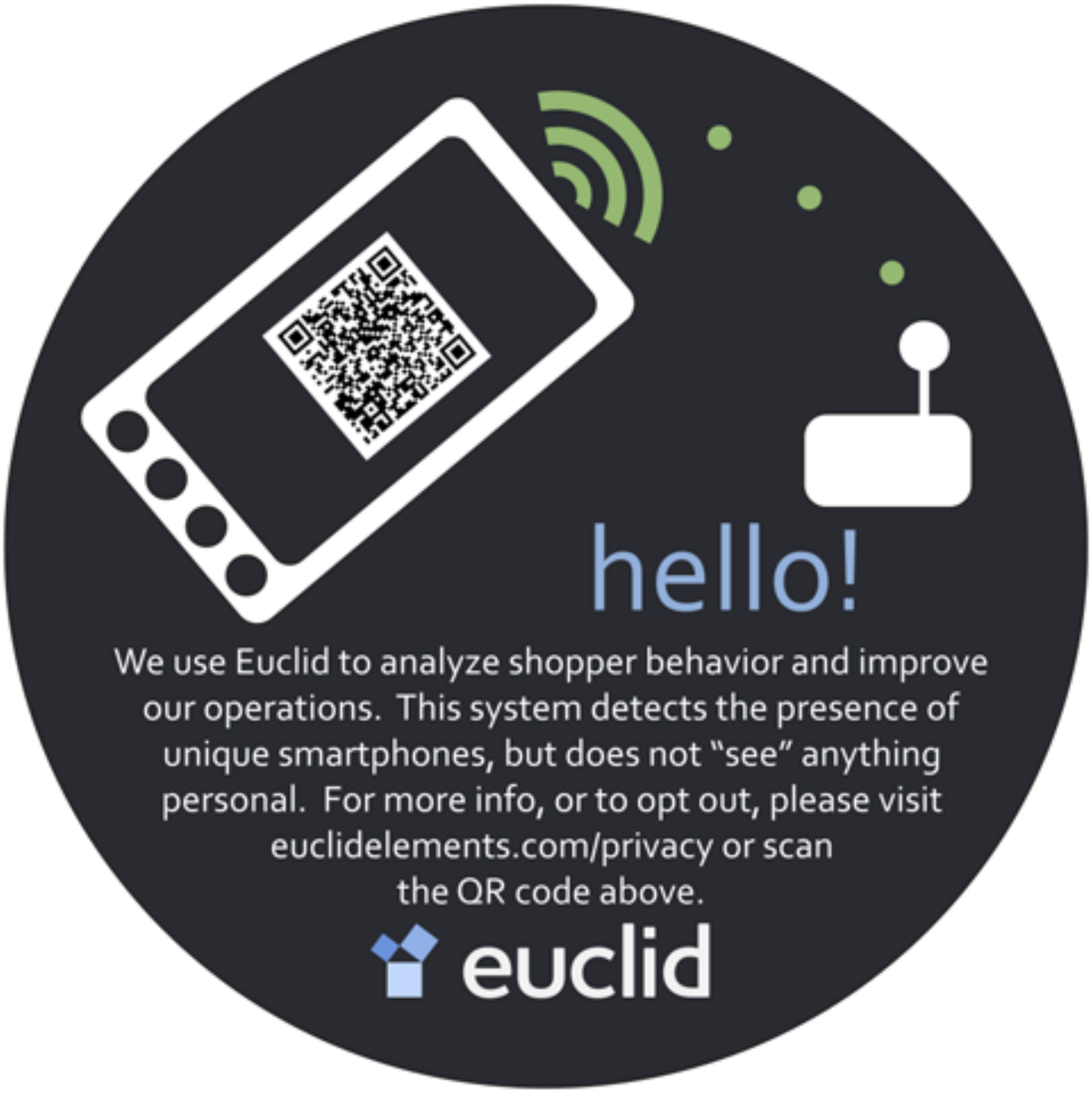
Sincerely,

Will Smith
CEO & Co-Founder, Euclid Inc.

Enclosures (2)

Euclid standard notice sticker

6-inch diameter



hello!

We use Euclid to analyze shopper behavior and improve our operations. This system detects the presence of unique smartphones, but does not "see" anything personal. For more info, or to opt out, please visit euclidelements.com/privacy or scan the QR code above.

euclid

1. Exactly how many unique smartphones has Euclid tracked in its clients' stores?

We have counted a total of 50 million Wi-Fi-enabled devices in our clients' stores, 93% of which are located in the United States. We do not receive the necessary information to determine specifically whether a device is a phone, tablet, or laptop. However, based on the movements of devices, we estimate that 70% of them are smartphones.

2. In what cities and states does Euclid track consumers' smartphones?

Please refer to Appendix I for a complete list of states and zip codes in which Euclid's system is currently in use.

3. Does Euclid track people's smartphones when they enter a store but don't buy anything?

Because our system is designed to protect consumer privacy, we have specifically prevented any linkage between data received by Euclid's sensors and a store's checkout system and customer database. Euclid has no information, whatsoever, on whether a device owner has purchased anything or not, and we have made sure that our system never receives information such as a consumer's name, address, phone number, or email.

Here is how Euclid's sensors work. Every smart device equipped with Wi-Fi (including mobile phones, laptops, tablets, and e-readers) has a unique identifier known as a MAC address. These devices regularly send out signals ("pings") that contain their MAC address to find Wi-Fi hotspots, such as those commonly found at coffee shops, airports, and in public spaces. When a shopper carrying a smart device walks by a retail store, the Euclid sensor at the store recognizes the broadcasted ping, scrambles the MAC address into what is known as a hash, discards the MAC address data, and sends the hashed value to Euclid's servers. In addition to the anonymous hash, the sensor also transmits basic device data received by our sensors: manufacturer code (Apple, Samsung, etc.), signal strength, and, if the device is currently connected to a specific Wi-Fi network, the name of that Wi-Fi network.

We use this anonymous data to derive aggregated insights about in-store traffic that are shared with the retailer. Because the pings are broadcasted periodically as the devices search for the presence of a Wi-Fi network, our system also can tell how long a device is in a particular store by comparing the time between the first ping and the last ping before the device leaves the store. This allows us to estimate the duration of shopper visits and allows our clients to determine, in aggregate, the percentage of visits that were likely too short to result in a sale.

A retailer using Euclid receives only anonymous, aggregated information such as: "Today 300 potential customers walked by your storefront and 150 entered. Of the 150, 15 percent stayed for less than 5 minutes, 55 percent stayed for 5-15 minutes and 30 percent stayed for longer than 15 minutes." The retailer can use these metrics to make intelligent decisions about staffing, merchandising, and displays that can dramatically affect their sales and profitability. However, we do not share any information between our clients, and all clients receive only anonymous, aggregated data.

Euclid improves the customer experience by helping retailers pinpoint specific ways to reduce wait times, extend business hours, and improve staffing levels. Using Euclid's tools, retailers can operate more efficiently, stay competitive, and serve their customers better.

4. Does Euclid track people's smartphones when they walk past a store without entering it?

Yes, Euclid's sensors receive the Wi-Fi signals that are broadcast by smart devices as they come into range in front of the store. However, once they leave the range of the store sensor, the signals are no longer received.

Measuring storefront traffic is important, as it allows us to show retailers how well they convert passers-by into visitors. For example, the retailer can use this data—which is always anonymous and aggregated—to compare the effectiveness of different window displays, helping them improve their performance and better compete with e-commerce stores.

5. Does Euclid track particular individual smartphone owners as they visit or walk past different stores?

Our clients typically place their sensors where they can recognize devices both inside and in front of their stores. This allows Euclid to estimate whether a potential consumer walking by the storefront actually enters or just passes by. If three adjacent stores are using the Euclid service, the sensor in each store would receive signals from the device. However, we do not share any information between our clients, and all clients receive only anonymous, aggregated data.

6. Euclid's online Privacy Statement says that its technology would enable it to tell a client whether "more people usually tend to grab a coffee or an ice cream after going to the dentist[.]" I understand that Euclid's technology is not being used in any medical facilities or pharmacies. Is that correct? If so, will Euclid pledge that it will never deploy its technology in or near any medical facilities or pharmacies in the future?

Euclid's technology currently is not being used in any medical facilities or pharmacies. We understand concerns about the sensitivities associated with healthcare data. In our view, this is some of the most sensitive data any business might possess, which is why we have designed our product to ensure that it does not run afoul of any of the important protections provided by HIPAA, the HITECH Act, or other United States privacy regulations.

Although we do not have current plans to deploy our product in medical facilities or pharmacies, we can envision a world where our technology could be used to help reduce healthcare costs, for example, by improving efficiency in emergency room waiting areas. If ever we are presented with a specific use case, we pledge that we will fully engage with your office on the development of any such plans, and that we will always remain 100% compliant with the law and committed to protecting customer privacy.

7. The Privacy Statement states that Euclid may augment its client reports with "information [Euclid] guesses infers [sic] from user activity, such as whether a device owner is male or female, income bracket, etc." (emphasis added). How exactly could Euclid guess or infer a consumer's gender and income bracket based on her smartphone data?

We understand the confusion this statement causes. What we mean is that we could make intelligent guesses based on our data, e.g., someone who spends time in a pet store may own a dog or a cat. However, we recognize that these can only ever be inferences.

While we included this sentence in our privacy statement in an effort to be as transparent as possible, in reality, this is not a service that Euclid offers currently. Should we ever decide to explore this capability, we commit to working closely with you to address any potential privacy concerns this may raise.

8. A recent *New York Times* article said that Euclid's technology is used to calculate "the percentage of people who come into the store who leave without making a purchase." How does Euclid calculate that percentage based on consumer smartphone data?

Please refer to our response to question three (3).

9. What mechanisms does Euclid have in place to monitor and identify breaches of consumer data?

Euclid recognizes the critical importance of data security in its service, and consults with many recognized security experts on an ongoing basis in our efforts to continually protect our product and associated data. One of the best defenses we employ is to limit the kind of data we receive to only the minimum necessary to provide our services: MAC address, manufacturer code (Apple, Samsung, etc.), signal strength, and, if the device is currently connected to a specific Wi-Fi network, the name of that Wi-Fi network.

We then scramble the MAC address into what is known as a hash, discard the MAC address data, and send the hashed value to Euclid's servers to prevent any possibility of unauthorized use. Access to the data is limited to authorized employees, and the data itself is deleted after 18 months.

Euclid cannot and never will receive any information relating to names, addresses, phone numbers, emails, etc. That information is not on our servers and therefore is never at risk for breach.

10. Has Euclid's consumer data ever been breached?

Euclid has had no reports of unauthorized access to, or breaches of, its databases.

11. The Privacy Statement says that Euclid's data is stored with Amazon Web Services. In January 2012, Zappos, an Amazon-owned company, suffered a breach that compromised the names, shipping and billing addresses, phone numbers, and email addresses of over 24 million customer accounts. Has Euclid taken additional precautions since this breach?

Please refer to our response to question nine (9).

12. If a law enforcement agency or a company told Euclid the MAC address for someone's smartphone and asked what stores the owner of that smartphone had previously walked past or visited, would Euclid be able to answer that question?

If the authorities provided the MAC address for a device, Euclid would only be able to determine whether the device had passed near one of its sensors by running it through the original hash function and then searching its databases for an identical hash result. Even if any matching information existed, we would only release it to a requesting agency if it complied with all necessary legal processes.

It's worth noting that we have never received a request for location information from the authorities. In our view, it is very unlikely that a law enforcement agency would ever turn to Euclid for location information since Euclid does not utilize GPS technology and our sensors are confined to a limited number of stores. Phone companies (and mobile apps with access to the device's GPS data) have a much more accurate and comprehensive location record for a specific device.

13. Will Euclid require law enforcement to obtain a warrant before disclosing a particular consumer's location records?

We would require a warrant or court order before disclosing the limited device location data that we possess.

14. Does Euclid have any plans to sell, rent or disclose any of its consumer data to data brokers or any other third parties?

We do not have any plans to sell, rent, or disclose any data to data brokers or any third parties.

15. Will Euclid assure users that it will never sell, rent or disclose any of its consumer data to data brokers or any other third parties?

We can assure users we will not sell, rent, or disclose any data to data brokers. It is hard to imagine all third parties that may have an interest in the basic device data that Euclid receives (for example, researchers might find the data useful in exploring an issue with larger societal implications). However, we would carefully consider and prioritize the privacy impact on device owners in making any decision about disclosing the limited device information we receive.

16. Will Euclid move to an "opt-in" model where a unique person is only tracked if she agrees to that tracking? If not, why not?

Because Euclid has limited the data received to exclude information such as names, phone numbers, email addresses, and shares this limited data only with its retailers in anonymous, aggregated form, we believe that the opt-out model is appropriate. With that said, your questions have led us to closely examine our product and work. Having an innovative product that helps both consumers and retailers is not enough. We support your efforts and we therefore renew our commitment to bringing value while striving to protect consumers and their right to privacy. To that end, Euclid reaffirms its commitments that protect consumer privacy:

- Our sensors receive only the following basic data: MAC address, manufacturer code (Apple, Samsung, etc.), signal strength, and, if the device is currently connected to a specific Wi-Fi network, the name of that Wi-Fi network.
- We cannot and never will receive any information relating to names, addresses, phone numbers, emails, etc.
- We never share information on individual devices.
- We never link data to specific individuals.
- We never share information between our clients.
- We provide a permanent opt-out process for any customer who wishes to do so. Our in-store notices direct customers to our website, which features a simple process by which customers can permanently opt out and delete data from our service.

In addition, Euclid makes the following new commitments to further protect consumer privacy:

- We will include posted customer signage as a stipulation in our contracts with all retailers going forward.
- We will institute a new and comprehensive education program about the opt-out process that we will require all retailers to undergo.
- We will strengthen our privacy policy to prohibit the sale, rental, or disclosure of any of Euclid's data to data brokers.
- We will create a formal policy outlining our requirements for a warrant or court order to comply with any request for data, which we will rely on in case we should ever receive such a request.

We welcome the opportunity to work with you and your staff, as well as others in the industry and the privacy community, to ensure real-world shopper insights always put consumer privacy at the forefront while helping to keep brick-and-mortar businesses competitive.

Appendix I: States and zip codes in which Euclid's system is currently in use

State	Zip codes
Arizona	85050, 85086, 85224, 85251, 85260, 85281, 85308, and 85705
California	90036, 90040, 90064, 90067, 90241, 90401, 90503, 90620, 90703, 90712, 91204, 91210, 92618, 92626, 92660, 92683, 92691, 92705, 92821, 92865, 92868, 93901, 94010, 94022, 94025, 94063, 94102, 94103, 94105, 94107, 94108, 94109, 94110, 94111, 94114, 94115, 94132, 94158, 94301, 94303, 94304, 94306, 94403, 94558, 94588, 94608, 94709, 94952, 94965, 95020, 95035, 95112, 95128, 95630, 95687, and 95815
Colorado	80206 and 80301
Connecticut	6810 and 6830
Florida	32714, 32771, 32803, 32809, 32819, 32821, 32839, 33139, 33180, 33323, 33428, 34741, 34787, and 34788
Georgia	30305
Idaho	83404
Illinois	60077, 60540, 60602, 60654, and 62208
Massachusetts	01760, 01923, 02116, 02139, and 02332
Maryland	21204
Minnesota	55425
Missouri	63021, 63044, 63123, and 63376
New Jersey	07043, 07078, 07201, 07702, 07728, 07753, 08002, 08096, 08527, 08723, 08822, and 08852
New York	10003, 10010, 10011, 10012, 10019, 10020, 10023, 10111, 10917, 10952, 11201, 11373, 11746, 11772, and 11901
Ohio	43240, 44446, and 44512
Oklahoma	74133
Oregon	97204
Pennsylvania	15061, 15084, 15123, 15146, 15205, 15220, 15237, 15301, 15601, 16127, and 19102
Tennessee	37601, 37862, 37919, 37924, and 37934
Texas	75061, 75225, 76117, 77056, 78006, 78028, 78163, 78223,

	78224, 78239, 78259, 78758, and 78840
Utah	84041, 84070, 84097, 84098, 84101, 84341, 84405, and 84601
Virginia	20166, 22182, 22202, 22314, and 22973
Washington	98101 and 98188
West Virginia	26330 and 26501