Kai Malcolm
Guidance from Dr. Luca Bonomi
BMIF 7380 - Project Interim Report
Vanderbilt University
04 / 08 / 2022

Introduction

From a Gallup poll conducted in 2019, over 1 in 5 US adults regularly wear a fitness tracker, devices which record biometric information such as heart rate (EKG), steps, and the different exercise intensities ranging from Very Active to Sedentary. A more popular device is the smartphone, which in many cases functions in a similar manner (captures and stores GPS location, accelerometer and gyroscope data, etc.) and is owned by over 294 million Americans (Kolmar, 2022). This conversation is also relevant to the explosive growth of AR and VR interfaces, which typically collect gaze, EEG, EMG, and/or gesture data. Wearable devices increase the convenience of quantifying health as well as making interaction with technology more fluid, but these benefits do not come without risks to user privacy. Today, only the tip of the iceberg for such data privacy risks has surfaced: for example, location information from activity trackers published by Strava.com (a platform similar to Fitbit, used for showing popular running routes by creating a heat map of users' routes) was used to identify US military bases abroad due to the predominantly American user base (Hern, 2018). From an NPR survey of 70+ domestic abuse shelters, 85 percent of shelters work with victims whose abusers tracked them using their smartphones' GPS, 75% have victims whose abusers eavesdropped on their conversation via hidden mobile apps, and over half of the shelters ban Facebook due to concerns about a stalker finding their location (Shahani, 2014).

Researchers have also been working to expose privacy threats inherent to this high-resolution, fine-grained, and intimate form of data collection: Alam (2021) found that breathing rate, heart rate, and hand gesture data can be utilized by attackers to re-identify user's identity from HIPAA compliant wearable data. Torre et al. (2018) found that in order to use a FitBit product or app, users are prompted to allow smartphone permissions including: identity, contacts, location, SMS, photos/media, camera, Bluetooth, and device ID/call information, with required inputs of name, gender, height, weight, and birthday, making this a minefield for reidentification. There are of course obvious implications if health insurance companies are able to re-identify health information and link to individuals using such leaked biometric data. More concerningly, Zhang et. al. have shown that popular EMG-based armbands can be used to recover sensitive information such as passwords typed on a keyboard and PIN sequence entered through a touchscreen with a mean success rate of 91% by determining the exact timing of finger movements. Given that wearables are expected to make larger inroads into our daily lives, future risks are more likely to occur and will also be larger in scale. It has been established in research that individual's biometric information (particularly with EEG for head-mounted wearables) changes little over the course of their life, and furthermore, that as more powerful machine learning and signal processing methods are derived, the abilities of data processing algorithms will greatly surpass today's information extraction capabilities, creating a conundrum for ensuring informed consent (Stanton et. al., 2016). The main focus of this project is on future reidentification using wearable data today to link to sensitive health information within medical research studies: this specifically applies to the privacy considerations of wearable data in both private and clinical databases, particularly when devices are hacked or when users grant unintended access / release their own data online.

Methods / Experimental Design

This project has its computational focus on traditional wrist wearables, although the issues addressed extend beyond to smartphones and future wearables that may not be in mass production yet

(such as smart clothing or more advanced human-computer interfaces), which may gather EEG, EMG, or other sensitive biometric data. The project has been divided into 3 main phases: 1) data processing, 2) standard privacy measure analysis, and 3) the design and evaluation of privacy solutions. Thus far, work has concentrated on the first two items, which has consisted of using a public FitBit database available on Kaggle ("moibus", 2020) of anonymized data (no demographic fields such as age/gender/etc.).

Once the data was obtained, two critical steps were required before linking could take place: first, to determine which data fields were of interest (in terms of which fields held the most information), and second, to determine the uniqueness of reidentification associated with the dataset. The largest combined dataset for all the users is the daily data readings (note that there are smaller files for hourly and minutely data for certain fields, but those have been ignored for now), which focuses primarily on calories, steps, and time spent in various intensities of activity. To determine the informational content of each field, the relative entropy (AKA KL-divergence) was computed, which is a measure of how different any two given probability distribution functions are. Probability distributions that are more different have higher relative entropies, indicating that more information can be obtained by including the aforementioned distribution, as opposed to one with a lower relative entropy. This method consisted of computing the relative entropy of each data field (e.g. calories, steps, etc.) when compared to each other data field (thus making a symmetric square matrix), and then taking the column-average for each data field in order to find the average relative entropy. The formula of KL-divergence is shown below:

$$D_{KL}(P \,||\, Q) \;=\; -\,\Sigma\left(P(x)\, log \frac{Q(x)}{P(x)}\right) \qquad \text{Eqn. 1}$$

In order to determine the uniqueness, a set of "test persons" was created, with each person having X attributes (values from the chosen data fields), where X is typically less than M, the number of attributes per person for each data field, and N, the number of people in the dataset. For a preliminary analysis, only one data field was chosen, and thus all X attributes come from that single datafield, but for a more in-depth study, multiple data fields would be chosen and the X attributes would come from all the listed fields (this is in progress). Each attribute x is pulled from the domain of the given datafield, in this case pulled from the union of all measurements for that data field across all users in the database. At this point, it is checked to see if all X measurements of the test person are included in any user within the dataset (in the corresponding data field): if so, the test person is denoted as compatible with that user. This analysis is repeated for each test person, at which point it can be compared to see how many test persons were compatible with each user in the original database: if it is ever the case that only one user is compatible with a test person, then the user is denoted as uniquely identified. Furthermore, instead of relying on all X measurements being direct matches, a threshold vector was introduced, such that each analysis over all test persons was conducted for each thresh value within the threshold vector, where it is only required that the difference between any data points in any user dataset and the test person set is less than the current thresh value (e.g. at a thresh of 0, this is a direct match as seen before, at thresh of 1, this is akin to matches being accepted that are +/-1 of the user's data values). Note that there is no mechanism to link the data to the original users (e.g. their real names) and that is not the intent of this study.

Results / Experimental Analysis

The first analysis conducted was to determine which attributes contained the most information, or, to determine which attributes were best suited for reidentification attacks. Figure 1 below shows the

information content of each data field, with the three most prominent (which were used for the uniqueness investigation) highlighted in red.

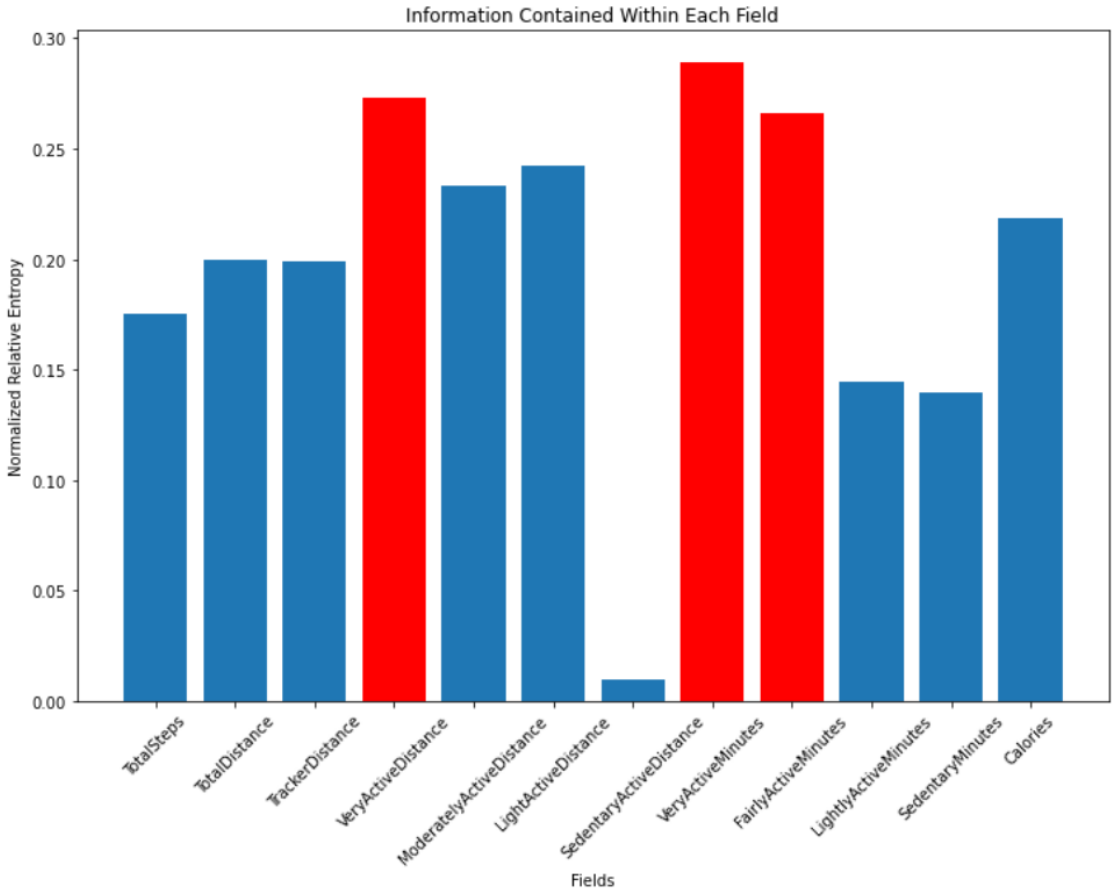

Figure 1: Exploration of most informative data fields.

The uniqueness is shown below in Figure 2. Note that there are a few clear trends: namely, as the number of values tested increases (e.g. the number of attributes each test person is given, in this case, from 1 to 3) there is a clear increase in the amount of uniqueness. With just 3 attributes per test person, a unique identification rate of over 90% can be achieved: now consider that wearables log data on the order of minutes, if not seconds or even more frequently. Second, there is a clear trend that when the threshold is relaxed from requiring a direct match to requiring being within plus or minus some threshold (in this case, 2 or 5), the uniqueness drops substantially. This is because a larger threshold means that there are more users who meet the condition (e.g. a larger threshold is akin to using larger bins, thus resulting in more matches and therefore less unique matches). Effectively, this is a form of increasing the coarseness of the data, as if all the data points were being smoothed to be indistinguishable from a group of data points that share a close Euclidean proximity. Of course, as the threshold is raised, the usefulness of the data necessarily declines (e.g. if the threshold is arbitrarily large, there is essentially only 1 bin and then everyone is the same, and there is no information to be gained from the system).

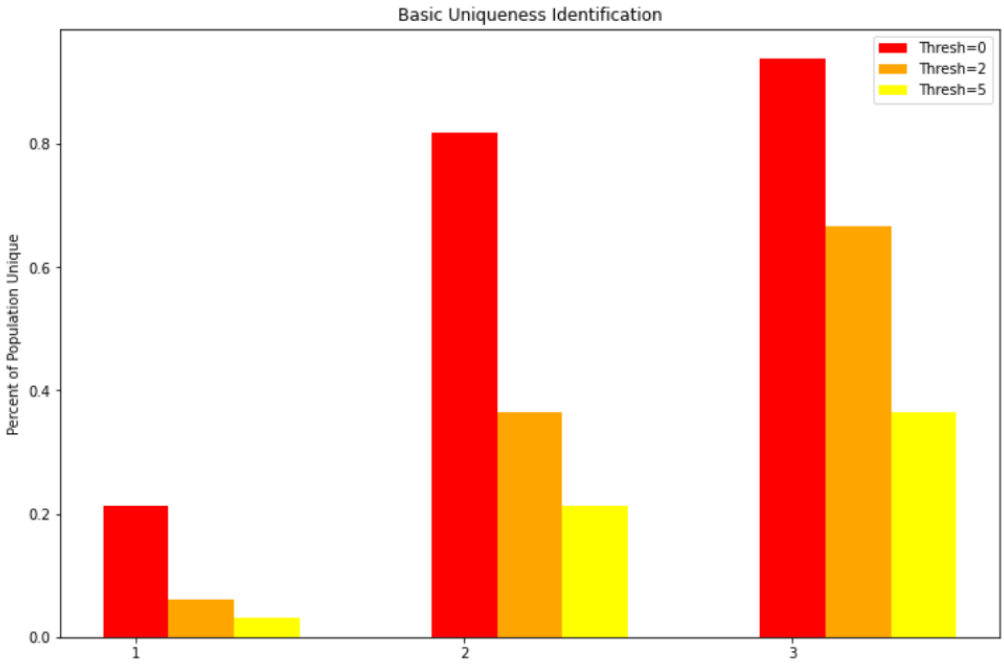

Figure 2: Exploration of user uniqueness.

Upcoming Work

Continuing from the uniqueness investigation above, a distance-based attack will be conducted in order to evaluate the privacy risk of the dataset. The final step of this project is to quantify the privacy risks beyond the preliminary analysis shown above: namely, this will take place by simulating an adversary who has obtained a subset of data. This data subset will be tested against the user dataset, exposing how many people the attacker can establish as part of the database, as well as how the attacker fares in terms of false positives: the adversarial model will be evaluated based on accuracy, precision, and recall. The goal of the attacker will mainly be to infer membership or to link records between databases, as knowing resting heart rate or daily activity may allow linkage to clinical databases that show other more sensitive qualities such as HIV or cancer diagnosis. As more private wearable products are introduced, more data will be generated and stored, which means more targets for attackers, showing that this is a real risk that will only grow with time.

The originally proposed timeline has been slightly altered, mainly in order to prioritize the empirical privacy risk measure using uniqueness and the aforementioned distance-based attack (with multiple attributes as opposed to the single column uniqueness investigation described above in the Methods section). The final step will be to assess the effectiveness of generalization (perhaps through increasing data coarseness mentioned above with respect to the thresholds) and standard differential privacy techniques in reducing the privacy risks. The door will be left often for data synthesis and full database sanitization (as a few papers have been identified that provide open source tools for these purposes), but these would only be extra items if the above focus on privacy risk measure and basic differential privacy risk mitigation techniques prove successful.

References

Alam, M. (2021). *PRI-attack: Person re-identification attack on ... - arxiv.org*. PRI-Attack: Person Re-identification Attack on Wearable Sensing. Retrieved from https://arxiv.org/pdf/2106.11900v1.pdf

Bernstein, D. (2020, August 5). *Texas Tech basketball abuse allegations show risk of Wearable Tech in sports*. Texas Tech basketball abuse allegations show risk of wearable tech in sports. Retrieved from https://www.sportingnews.com/us/ncaa-basketball/news/texas-tech-abuse-allegations-wearable-tech-in-sports/1lan1crzqlel81wxloz0ibzqjr

Burt, C. (2022, March 31). *Evidence of Taliban attempting biometric searches leaves data access unclear: Biometric Update*. Evidence of Taliban attempting biometric searches leaves data access unclear. Retrieved from https://www.biometricupdate.com/202203/evidence-of-taliban-attempting-biometric-searches-leaves-data-access-unclear

Hern, A. (2018, January 28). *Fitness tracking app Strava gives away location of secret US Army Bases*. The Guardian. Retrieved from https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Kolmar, C. (2022, January 30). *U.S. smartphone industry statistics [2022]: Facts, growth, trends, and forecasts*. Zippia. Retrieved from https://www.zippia.com/advice/us-smartphone-industry-statistics/

Landau, O., Cohen, A., Gordon, S., & Nissim, N. (2020, April 21). Mind your privacy: Privacy leakage through BCI applications using machine learning methods. Retrieved from https://www.sciencedirect.com/science/article/pii/S0950705120302641

Lehto, M., & Lehto, M. (2017). *ECCWS 2017 16th European conference on cyber warfare and security*. Health Information Privacy of Activity Trackers. Retrieved from https://books.google.com/books?hl=en&lr=&id=uFA8DwAAQBAJ&oi=fnd&pg=PA243&dq=Lehto%2C%2BM.%2C%2B%26%2BLehto%2C%2BM.%2B%282017%29.%2BHealth%2Binformation%2Bprivacy%2Bof%2Bactivity%2Btrackers.%2BProceedings%2Bof%2Bthe%2B16th%2BEuropean%2BConference%2Bon%2BCyber%2BWarfare%2Band%2BSecurity.%2BUniversity&ots=YTr1iDYl4D&sig=S27ohiaJGMDZSZNE5SBSy4UtUUI#v=onepage&q&f=false

McCarthy, J. (2021, November 20). *One in five U.S. adults use health apps, Wearable Trackers*. Gallup.com. Retrieved from https://news.gallup.com/poll/269096/one-five-adults-health-apps-wearable-trackers.aspx

moibus. (2020, December 16). *Fitbit Fitness Tracker Data*. Kaggle. Retrieved from https://www.kaggle.com/datasets/arashnic/fitbit

Shahani, A. (2014, September 15). *Smartphones are used to stalk, control domestic abuse victims*. Smartphones Are Used To Stalk, Control Domestic Abuse Victims. Retrieved from https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims

Stanton, S. J., Sinnott-Armstrong, W., & Huettel, S. A. (2016, February 17). *Neuromarketing: Ethical Implications of its use and potential misuse - Journal of Business Ethics*. SpringerLink. Retrieved from https://link.springer.com/article/10.1007/s10551-016-3059-0

Torre, I., Sanchez, O. R., Koceva, F., & Adorni, G. (2017, August 29). *Supporting users to take informed decisions on privacy settings of personal devices - personal and ubiquitous computing*. SpringerLink. Retrieved from https://link.springer.com/article/10.1007/s00779-017-1068-3

Zhang, R., Zhang, N., Du, C., Lou, W., Hou, T., & Kawamoto, Y. (2017, October). *A from electromyogram to password: Exploring the ... - CNSR@VT*. From Electromyogram to Password: Exploring the Privacy Impact of Wearables in Augmented Reality. Retrieved from https://www.cnsr.ictas.vt.edu/publication/tist_zhang.pdf