

NetChoice *Promoting Convenience, Choice, and Commerce on the Net*

Carl Szabo, Policy Counsel
NetChoice
1401 K St NW, Suite 502
Washington, DC 20005
202-420-7498
www.netchoice.org



June 9, 2014
SUBMITTED ELECTRONICALLY
Federal Trade Commission

NetChoice Public Comments to FTC on workshop on Consumer Generated and Controlled Health Data on May 7, 2014

NetChoice respectfully submits the following comments regarding the Federal Trade Commission (“FTC” or “Commission”) workshop on Consumer Generated and Controlled Health Data.

NetChoice is an association of leading e-commerce and online companies, plus thousands of small businesses that rely on e-commerce. We work to promote the integrity and availability of the global internet and are significantly engaged in privacy issues in the states, in Washington, and in international internet governance organizations.

Privacy-related laws that specify how data can be collected, used, and shared can create barriers to legitimate online commerce. NetChoice has a long history of breaking down regulatory barriers, beginning with helping travel agents, contact lens suppliers, and real estate brokers whose online innovations clashed with legacy regulations that protect traditional business models.

The modern Hippocratic oath says, first “Do No Harm.” We ask the FTC to take this same approach when addressing privacy issues surrounding consumer generated and controlled health data, especially in the form of mobile health data.

Consumer generated health data can create unfathomable benefits for consumers such as encouraging consumers to eat better and exercise, helping doctors remotely diagnose patients and monitor their medicine, and identifying viral outbreaks before they become epidemics.

The Hippocratic oath says, first “Do No Harm.” The FTC should take the same approach when addressing privacy issues surrounding mobile health apps.

While policymakers are clearly aware of these benefits, we worry that current discussions about consumer generated health data are focusing mainly on the hypothetical harms of health data. This imbalance could lead consumers to mistakenly avoid adoption of useful tools and encourage unnecessary regulation – both of which will stymie the growth of consumer generated data and its biggest potential, mobile health applications.

Consumers have adopted online applications and services at an unprecedented rate when compared to previous new technologies. Moreover, research shows that advertising and marketing practices are not making consumers more reluctant to go online. In fact, it is quite the opposite. A recent study showed that the amount of consumption time spent online continues to increase even as online advertising

expands.¹ While we agree that generated data, especially sensitive health data, should be securely protected, any approach from government should avoid dissuading consumers from enriching their lives (and improving their health) through online services.

Thus, to avoid creating stigmas about mobile health apps, we make the following recommendations to the FTC:

1. The FTC should recognize that not all health apps should be treated the same; privacy obligations should allow for context specific FIPPs.
2. The FTC should examine how existing laws and regulators already operate in this space.
3. The FTC should further research deidentification with relations to health information. If problems are found, the FTC should make recommendations about how to improve the privacy.

Benefits of mobile health apps

We agree with Commissioner Brill's comments² that we should discuss the benefits of mobile health. Unfortunately, the Consumer Generated and Controlled Health Data workshop ("Workshop") seemed to spend considerably more time on the theoretical harms. Such focus makes easier the dismissal of a useful and beneficial technology. However, there are substantial benefits to consumer awareness and health made possible by this new technology.

MOBILE HEALTH APPS ENCOURAGE BETTER HEALTH

A recent poll found that "73 percent of respondents believe they are healthier today, thanks to their use of mobile technology to track health and fitness" and "70 percent are using mobile apps daily to monitor calorie intake and physical activities. 69 percent believe using mobile technology to track their health and fitness is actually more important than using their smartphone for social networking or mobile shopping."³

73% of survey respondents believe they are healthier today, thanks to their use of mobile technology to track health and fitness

The FTC should avoid creating rules or guidelines that would curtail the development of these beneficial tools for Americans' health.

Consumer Health Logging

By merging health with devices that we carry at all times – watches, step counters, and cell phones – consumers are using new tools to become healthier. Some of this motivation is simply monitoring – much of which is nothing new, but is made easier through online innovation.

Consider the "Jenny Craig Weight Loss Program." Historically, users would use pocket lists and write their meals in handbooks. Unfortunately, this created a barrier to success. Sometimes it was too complicated, or users simply forgot to log the meal. A mobile app provides the same logging features, but on a device they always have with them and one that easily calculates points.

¹ Mary Meeker, Internet Trends 2014 – Code Conference (May 28, 2014), available at kpcb.com/InternetTrends

² Commissioner Julie Brill, Transcript of Consumer Generated and Controlled Health Data Presentation (May 7, 2014)

² Commissioner Julie Brill, Transcript of Consumer Generated and Controlled Health Data Presentation (May 7, 2014)

³ Mobyquity, *New Research: 55 Percent of Health and Fitness Mobile App Users to Add Wearables*, May 8, 2014, available at <http://www.mobyquityinc.com/new-research-55-percent-health-and-fitness-mobile-app-users-add-wearables>

The Withings app provides a functional way to track blood pressure, to the benefit of doctors and their patients. It can be difficult to remember to check and keep accurate logs of blood pressure. Moreover, patients may forget to bring such logs to their doctors. The Withings app shows mobile alerts to remind patients to check their blood pressure and keeps detailed logs on the patient’s smartphone – something they carry when visiting their doctor.

Withings blood pressure monitor makes monitoring easier and more accessible to users and their doctors



Walking provides well-documented health benefits. While pedometers are nothing new, the growth of digital pedometers like the FitBit, Jawbone Up, and cellphone-based pedometers have moved consumers off the couch into a healthier lifestyle. A Mayo Clinic study found that “changes in behavior [inspired by mobile health apps] can be an important boon to the overall health of sedentary people.”⁴ Seeing the results

online and competing with friends can further encourage consumers to get-up and walk.

“Gameification” of health practices provides benefits similar to a workout partner. Encouragement and competition are important motivators for getting out for a run or doing a workout, and working out with friends is a proven motivator.⁵ Mobile health apps can overcome physical distance and barriers between workout partners. And this same approach of seeking the “high score” used in arcades can improve consumer health. For example, the Nike Running App users can challenge friends to beat their time or distance. PushUps app users can try to outdo each other’s records.

Telemedicine

Telemedicine is more than a buzzword -- it is now a reality. Consumers across the country are enjoying more choices in health care while doctors are able to monitor and diagnose patients without requiring them to come to the office. Medical apps like the Medicare Blue app, and Innovate Wireless Health, consumer-monitoring tools like the Withings Blood Pressure app, and startups like AngelMD are bringing doctors to people.

Telemedicine, powered by mobile health apps, breaks down barriers for patients. No longer limited by geography, consumers now have a greater choice of doctors – promoting an increase in health care competition that has long been an important goal for the Commission. And mobile health apps allow users to

FitBit app helps users encourage friends to be more active

Friends			
7 Day Step Total			
1		Elizabeth C.	94,419 >
2		You	71,353 >
3		Tina	71,069 >
4		Nick	65,474 >
5		Michael N.	57,727 >

⁴ Coleen Curry, *Fitness Trackers: Step by Step to Better Health or Driving Us Crazy?*, ABC News (Aug. 13, 2013), available at <http://abcnews.go.com/Technology/fitness-trackers-step-step-health-driving-us-crazy/story?id=19936093>

⁵ Lisa Freedman, *Six Reasons to Workout with a Partner*, Mens Fitness, available at <http://www.mensfitness.com/training/six-reasons-to-workout-with-a-partner>

take their records with them and see doctors they otherwise wouldn't have access to.

Mobile health apps can lower health care costs by allowing doctors to remotely monitor and diagnose patients. For example, Isansys' Patient Status Engine includes a wireless chest patch that monitors the patient's ECG, heart rate, respiration rate, and heart rate variability. Additionally, the package comes with a blood pressure cuff and a pulse oximeter that can share their readings for easy access from a computer, tablet, or smartphone. This device sends doctors immediate test results and eliminates the cost and time for a trip to the hospital.



Mobile health apps help consumers in remote areas. Consider the farmer that lives hundreds of miles from the nearest major hospital. Rather than losing days of time for each check-up, mobile health apps allow the farmer to see their doctor remotely and allow the doctor to monitor the farmer's health.

Finally, by using mobile health apps for medical monitoring and record keeping, consumers improve the quality of their records. As explained at the Workshop, Humetrix helps patients review their medical records and correct errors. Likewise, the PersonalRN app helps educate family members about patient situations.

The FTC should avoid forestalling these consumer benefits.

Identifying Epidemics

History is replete with devastating disease and sickness outbreaks. However, due in part to mobile health apps, we can better identify an emerging problem before it becomes a full-blown epidemic.

Take, for example, Google Flu Trends. By anonymously counting searches for "flu" and flu-like symptoms and the location of the search on mobile devices and through websites, Google provides useful data to health departments around the world.⁶ This information helps direct care to places with the greatest need. In fact, one report found Google Flu Trends was able to predict regional outbreaks of flu up to 10 days before they were reported by the Centers for Disease Control and Prevention.⁷ Likewise, Boston Children's Hospital analyzed Wikipedia's traffic to help predict flu trends in the state up to 2 weeks earlier than the CDC.⁸

These tools also help researchers. A 2013 John Hopkins research report said that Google Flu Trend data "was the only source of external information to provide statistically significant forecast improvements over the base model." Moreover, when combined with CDC information the research becomes even more beneficial.

The FTC should avoid stifling the development of these tools – especially as the world becomes more connected enabling viruses in one part of the world to jump to another.

Privacy Policies for Mobile Health Applications

Privacy policies are important, especially when addressing sensitive information like health information. Some argue that privacy policies alone are not effective, and many companies have responded with

⁶ Google Flu Trends - <http://www.google.org/flutrends/about/how.html>

⁷ Miguel Helft, *Google Uses Searches to Track Flu's Spread*, NY Times (Nov. 11, 2008)

⁸ Ryan Parrish, *New model predicts flu trends using Internet traffic on Wikipedia articles*, VaccineNews (Apr. 23, 2014)

more “just-in-time” notice when appropriate. Nonetheless, we want to inform consumers, not confuse them with a parade of intended and potential uses and we want to avoid strict limits that prevent the future use of data in ways that enhance consumer welfare.

EXISTING LAW ALREADY REQUIRES APPS TO HAVE PRIVACY POLICIES

FTC Section 5, FDA regulation, and state laws like the California Online Privacy Protection Act (CalOPPA),⁹ provide regulators with ample authority to compel mobile health app developers to develop useful and comprehensive privacy policies.

Under the California Attorney General interpretation of CalOPPA any mobile application that may impact a California consumer that collects personal user data must conspicuously post a privacy policy detailing, clearly and completely, how the application collects, uses, and shares personal data. In effect, all apps are subject to the CalOPPA privacy policy rules. And of course this includes mobile health apps.

In late 2012, the California AG began taking enforcement actions against apps for not having privacy policies. The AG sent out a wave of notifications to 100 companies in October 2012, warning app developers to post privacy policies or risk fines as high as \$2,500 per app download.¹⁰ The AG then took action against mobile app developers, including Delta Airlines.¹¹

FTC statements show the agency believes it has enforcement authority against an app for lack of a privacy policy, or one that fails to disclose material information.¹² And the FTC is aggressively on the beat when it comes to mobile apps not abiding by their privacy policies. Last year, the FTC took action against Path,¹³ Goldenshores Technology, and most recently SnapChat¹⁴ for collecting information outside the scope of the privacy policy. And the FTC settlement with Fandango and Credit Karma further showed that promises made in privacy policies extend to the security of information transmitted and stored.¹⁵ Clearly, the FTC already has the legal authority it needs to regulate mobile apps, including mobile health apps.

The Department of Health and Human Services (HHS) and Food and Drug Administration (FDA) are already involved in the regulation of mobile health apps. For example, the FDA issued guidance regarding the regulation and certification of mobile health apps, stating, “The FDA is taking a tailored, risk-based approach that focuses on the small subset of mobile apps that meet the regulatory definition of ‘device’ and that: are intended to be used as an accessory to a regulated medical device, or transform a mobile platform into a regulated medical device.”¹⁶

Regulation of mobile health apps exists and developers are responding to improve their privacy policies.

⁹ The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579

¹⁰ Press Statement, *Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law*, California AG Office (Oct. 30, 2012), available at <http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance>

¹¹ Press Statement, *Attorney General Kamala D. Harris Files Suit Against Delta Airlines for Failure to Comply with California Privacy Law*, California AG Office (Dec. 6, 2012), available at <http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-files-suit-against-delta-airlines-failure>

¹² See e.g., *Sears Holdings Mgmt. Corp.*, Docket No. C-4264, File No. 0823099 (Fed. Trade Comm'n Sept. 9, 2009) (decision and order), available at <http://www.ftc.gov/os/caselist0823099/090604searsdo.pdf>

¹³ Press Statement, *Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books*, FTC (Feb. 1, 2013), available at <http://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived>

¹⁴ Snapchat Inc., Docket No. C-4264, File No. 1323078 (Fed. Trade Comm'n) (decision and order), available at <http://www.ftc.gov/system/files/documents/cases/140508snapchatorder.pdf>

¹⁵ Press Statement, *Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers By Failing to Securely Transmit Sensitive Personal Information*, FTC (Mar. 28, 2014)

¹⁶ Food and Drug Administration, *Mobile Medical Applications* (10/23/13).

INUNDATING CONSUMERS WITH ADDITIONAL NOTICE COULD LEAD THEM TO STOP USING MOBILE HEALTH APPS

As stated above, we believe that transparency and informing consumers of their privacy is paramount, especially when using mobile health apps. However, we must avoid regulations resulting in apps overwhelming consumers with too many notices. If so, this overnotification could lead to desensitization to important notices and avoidance of beneficial technology.

In its DotCom Disclosure report the FTC acknowledged the desensitization threat: “Some consumers may not read information in pop-up windows or interstitials because they immediately close the pop-ups or move to the next page in pursuit of completing their intended tasks.”¹⁷ We have similar concerns. If required to show too many notices through mobile health apps, consumers may stop reading the notices and miss the notices that are of most importance.

The alternative to consumers ignoring notices is that they stop using the tool. If regulations result in excessively burdening the consumer experience, consumers may just avoid using mobile health apps depriving them of its benefits.

“Health apps” is Not A One-Size-Fits-All Category

NetChoice supports a “privacy by design” approach driven by customer preferences, not government regulation. Online businesses know that consumer confidence is essential and thus have sufficient incentive to meet consumer expectations.

Businesses must maintain the ability to set and experiment with defaults for information sharing without reprisal from government agencies and state AGs. Otherwise, new product development will suffer, and ultimately harm consumers and competition.

In keeping with the spirit of “privacy by design” mobile health apps should adjust their privacy application based on the information collected and how it is used.

Different information should be treated differently. This makes sense as apps that access less sensitive personal information should be treated differently than those that access a consumers’ entire medical history. Unfortunately, research by the Privacy Rights Clearinghouse *Mobile Health and Fitness Applications and Information Privacy* (“PRC Report”) suggested that running apps are “health apps” in the same way that one that stores medical records.

The Aetna app would receive the strictest application of FIPPs while Withings apps received a lower application and the Nike Running app a much lower one



Aetna Health app collects information from users and gives users access to their health records and claims



Withings App tracks user's blood pressure and weight



Nike Running app allows users to enter their height, weight, and shoe size

¹⁷ Fed. Trade Comm'n, *.com Disclosures: How to Make Effective Disclosures in Digital Advertising*, p. 4 (Mar 13, 2014), available at <http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf>

Contextual Application of FIPPs

Contextual application incorporates the notion that the more sensitive the information, the stricter the application of the Fair Information Practice Principles (FIPPs). For example, in the context of the Aetna health app, the contextual application of FIPPs should be strong.

NetChoice supports the FIPPs. In addition, given the differences in information collection and use among health apps, we endorse a contextual application of the FIPPs as suggested by Commissioner Ohlhausen.¹⁸ Note that this approach is not an abandonment of FIPPs but instead a contextual application.

We Disagree With Aspects of the FTC Presentation

We disagree with several aspects of the FTC Presentation “*Health Data Flows*” by Latanya Sweeney, Chief Technologist, FTC (“Presentation”).

We also worry that the flaws in FTC Staff’s Preliminary Observations “*A Snapshot of Data Sharing by Select Health and Fitness Apps*” (“Staff Observations”) will lead the FTC into improper regulation and/or discourage evolution of useful tools for consumers.

MOBILE HEALTH AND FITNESS APPS DO PROTECT USER PRIVACY

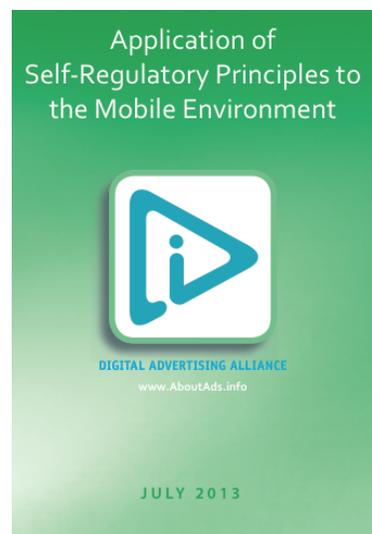
The second slide of the Presentation quoted the flawed PRC Report by saying: “mobile health and fitness applications are not particularly safe when it comes to protecting user privacy.” Not only is this statement false, but also several self-regulatory and administrative resources exist to prevent improper treatment of user data.

App Developers Do Care About Protecting User Privacy

In 2012, the FTC found that over sixty percent of apps had privacy policies. This was before the California AG stated that all apps must have privacy policies. Less than 2 years later, that number is over seventy-five percent¹⁹ and increasing.

Consumers hold apps accountable for privacy practices when they choose not to download an app. A recent TrustE survey showed 78 percent of consumers will not download an application that they do not trust and 40 percent of smartphone users check whether an app has a privacy policy.²⁰ Moreover, app store reviews give consumers a platform to rank and discuss an app’s privacy treatment. App developers are incentivized to take these responses seriously, since lower scores result in fewer downloads.

Expanding beyond web-based privacy, industry groups now provide mobile-based self-regulatory programs. For example, the Advertising Option Icon now applies to mobile platforms.²¹ Issued last summer, the “*Self-Regulatory Principles to the Mobile environment*” provide mobile app developers a



¹⁸ “I believe FIPPs remains a solid framework and is flexible enough to accommodate a robust big data industry, but we have some work to do to resolve these tensions.” Remarks of Maureen K. Ohlhausen1 Commissioner, *The Power of Data*, Georgetown University McCourt School of Public Policy and Georgetown Law Center (Apr. 22, 2014), available at http://www.ftc.gov/system/files/documents/public_statements/299801/140422georgetownbigdataprivacy.pdf

¹⁹ New Zealand Privacy Commission, *Mobile apps under the spotlight – global survey* (May 9, 2014) available at <http://privacy.org.nz/news-and-publications/statements-media-releases/mobile-apps-under-the-spotlight-global-survey/>

²⁰ Chantal Tode, *Venable attorney claims marketers must balance privacy concerns with consumer needs*, MobileMarketer (Mar. 14, 2014), available at <http://www.mobilemarketer.com/cms/news/legal-privacy/17380.html>

²¹ Application of Self-Regulatory Principles to the Mobile Environment, DAA, available at http://www.aboutads.info/DAA_Mobile_Guidance.pdf

framework for compliance and application of privacy policies to their apps. This includes purpose limitation, security, and accountability.

METHODOLOGICAL FLAWS IN PRC RESEARCH

Many of FTC staff's findings and statements in the Presentation came from the PRC Report. Unfortunately, this report is plagued with methodological flaws that result in flawed conclusions.

First, the PRC Report recognizes that "since any definition of risk is subjective and individual, we acknowledge an unavoidable *bias in our research*."²² However, this bias was not mentioned during the Presentation. Instead the Presentation focused on conclusory PRC Report statements that shed a negative light on mobile health apps.

Second, the PRC Report treated all mobile health apps the same. As discussed above, mobile health apps cover a wide spectrum of personal information. Nonetheless, by flooding its study with apps collecting less sensitive information, the PRC Report results skewed to make apps appear less privacy-sensitive than they are otherwise.²³

METHODOLOGICAL ISSUES IN FTC STAFF'S PRELIMINARY OBSERVATIONS

We appreciate the FTC's attempt to look deeper at this industry through an empirical approach. However, FTC Staff Observations were both undersized and skewed, and should not have been the basis for so much of the Workshop's discussions.

Lack of Focus on Harms

The FTC says "[u]njustified consumer injury is the primary focus of the FTC Act."²⁴ However, the FTC spent little time at the Workshop identifying actual harms or injuries sustained by consumers. While it is easier to hypothesize about potential misuse of mobile health apps, the FTC missed an opportunity to discuss *actual* harms and how to prevent and/or remedy them.

Identification of real harms drives solutions. But just talking about theoretical problems usually divides stakeholders and unnecessarily scares consumers. We recommend the FTC research examples of actual harm and focus on that discussion.

Flaws in Research of App Privacy

The Staff Observations research used a very small sample size—only 12 apps. With over 31,000 mobile health apps,²⁵ the sample size of the Staff Observations represents a mere 0.04% of the market – too small to draw the broad conclusions shown in the Presentation.

The Staff Observations stated that sharing by mobile health apps was very high. However, the methods used for the study skewed towards this high sharing. First, "if an app asked [] for permission to access a certain feature or to sync with another app, *we always accepted and opted in*."²⁶ This, of course, would lend itself to increased sharing, and the reality of actual sharing could in fact be much lower. Second, the Staff Observations made the same mistake as the PRC Research by treating all mobile health apps equally. By looking mostly at "two exercise apps, two dietary and meal apps, three system checker app"

²² Presentations of Consumer Generated and Controlled Health Data Presentation (May 7, 2014) (emphasis added).

²³ Only 84% of the free apps analyzed in the PRC Study were something other than "high risk." See Privacy Rights Clearinghouse *Mobile Health and Fitness Applications and Information Privacy*

²⁴ Federal Trade Comm'n, *FTC Policy Statement on Unfairness*

²⁵ Michael Essany, *Mobile Health Care Apps Growing Fast in Number*, mHealthWatch (Apr. 15, 2013), available at <http://mhealthwatch.com/mobile-health-care-apps-growing-fast-in-number-20052/>

²⁶ Latanya Sweeney, Transcript of Consumer Generated and Controlled Health Data Presentation (May 7, 2014)

it's likely that sharing might be greater as the sensitivity of the information is low — device info, gender, dietary information, etc.

Finally, the Staff Observations' "[d]id not review privacy policies"²⁷ of the apps. It would seem that if the staff were to use a very small sample of health apps to present findings suggesting threats to user health data, it should at least look at what those apps say about users' privacy.

Incorrect Information Regarding Re-Identification via Apps

The Staff Observations suggested that third parties could easily combine user data from different apps²⁸ -- reidentifying information across different apps. This isn't the case.

Each app uses its own unique identifier even when on the same smart phone. This means that the unique identifier for the Nike App is different from the unique identifier for the Aetna app. In essence, a third-party can't easily combine data from different apps. This makes the Staff Observations about reidentification and aggregation specter unlikely to be a real threat.

Staff Observations Suggest Disallowing Deidentified Data

Citing the integration of deidentified hospital data with public records, the Staff Observations suggest removing the possibility of using deidentified data because it might be reidentified. We understand the concerns, however, this question goes directly to use of data rather than prohibiting collection.

Publicly available state health databases provide researchers with useful information. It helps identify changes in health patterns, track disease epidemics, and find ways to lower medial costs.²⁹ None of this is mentioned in the Presentation. Instead the Presentation focused on potential misuses of data.

Rather than letting the perfect be the enemy of the good, we ask the FTC to give advice on how to improve deidentification to make it more effective – perhaps establishing a standard for deidentification or looking at restrictions on reidentifications.

Recommendations for FTC

1. The FTC should recognize that not all health apps should be treated the same; privacy obligations should allow for context specific FIPPs.

As discussed above, the sensitivity of information collected should dictate the level at which the FIPPs are applied. We take issue with the treatment of mobile health apps as a "one size fits all." Much of the Workshop and Staff Observations treat all mobile health apps the same rather than appreciating that different standards should apply for different collected information. For example, it does not make sense to treat a Nike Running App in the same manner as the Aetna Health App.

We recommend the Commission recognize that not all health apps should be treated the same and the privacy obligations should allow for context-specific FIPPs.

2. The FTC should examine how existing laws and regulators already operate in this space.

As noted above, between existing FTC authority, regulations from the states, and the work of other agencies like HHS and FDA, there are already laws and enforcers in place to regulate mobile health apps.

²⁷ Presentation of Consumer Generated and Controlled Health Data Presentation (May 7, 2014)

²⁸ *Id.*, "There are implications where health contains dietary habits and circumstances are being Aggregated using identifiers unique to a person or their device."

²⁹ For example, the University of Pennsylvania is using the publicly available health data to analyze the effect of the Affordable Care Act. <http://www.rwjf.org/en/grants/grant-records/2013/11/monitoring-the-affordable-care-act-by-creating-a-publicly-availa.html>

Rather than create new rules and regulations, we ask the FTC to follow the recommendation of Commissioner Ohlhausen to see if existing rules accomplish the objectives the FTC seeks:

Before seeking new privacy legislation, it is important to identify a gap in statutory authority or to identify a case of substantial consumer harm that we'd like to address, but can't, with our existing authority, especially given the array of financial, medical, and health and safety harms already reachable under our current FTC authority or other laws. Otherwise, it is difficult to tell whether the additional protections are necessary or will, on balance, make consumers better off because information sharing has benefits for consumers such as reducing online fraud, improving products and services, and increasing competition in the market overall.³⁰

Before looking to create any rules, regulations, or guidance, the FTC should review the existing statements and actions from other federal and state agencies.

3. The FTC should further research deidentification with relations to health information. If problems are found, the FTC should make recommendations about how to improve the privacy.

Researchers rely on publicly available state health databases. If the FTC finds that current deidentification of publicly available state health databases inadequate then we ask the FTC to make recommendations on ways to improve the deidentification process.

The FTC can help lead states towards a better deidentification process by outlining best practices for deidentification and identifying uses that should be avoided.

We thank you for your consideration and ask that you recognize the impact FTC regulation could have on growing or limiting these wonderful and exciting new health innovations.

Sincerely,

Carl M. Szabo
Policy Counsel, NetChoice

NetChoice is trade association of leading e-commerce and online businesses. www.NetChoice.org

³⁰ FTC Commissioner Maureen K. Ohlhausen Speech Before the Hudson Institute, *The Government's Role in Privacy: Getting it Right*, (October 16, 2012).