Submitted via overnight delivery / email to https://ftcpublic.commentworks.com/ftc/privacyconresearch

October 9, 2015

Federal Trade Commission
Constitution Center
400 7th St SW
Washington, DC 20024

Re: FTC PRIVACYCON Call for Presentations

I appreciate the opportunity to submit my research entitled ***Data privacy in an age of increasingly specific and publicly available data: An analysis of risk resulting from data treated using Anonos' Just-In-Time-Identity Dynamic Data Obscurity methodology***, a copy of which is attached.

This letter is separated into the following two sections:

I. Proposal to Present Research on Dynamic Data Obscurity; and
II. History of the Term Dynamic Data Obscurity.

I. Proposal to Present Research on Dynamic Data Obscurity

I propose to present my research on Dynamic Data Obscurity at the FTC conference on January 14, 2016 as an example of an important recent trend related to consumer privacy and data security.

Dynamic Data Obscurity involves temporally dynamic data obscuring technology that actively limits the risk of re-identification. Static de-identification techniques suffer from numerous shortcomings. Dynamic obscuring technology helps retain data privacy while reducing risks involved in collecting, storing, processing, and analyzing data. Specifically, it turns data into business intelligence (BI)[1] by transforming static access controls into technologically-enforced dynamic permissions applied per-element, instead of broadly across individuals, entire records, or applications. This maximizes the utility of underlying data by allowing intelligent, adaptable, and compliant permissions while fundamentally enforcing core protections against personally identifiable or sensitive information.

[1] Business intelligence (BI) is an umbrella term that includes the applications, infrastructure and tools, and best practices that enable access to and analysis of information to improve and optimize decisions and performance. See http://www.gartner.com/it-glossary/business-intelligence-bi

Technologically-enforced Dynamic Data Obscurity rules can account for access, use, display, time, and location restrictions, across any industry or regulatory standard, thereby helping to overcome shortcomings of static de-identification such as the following:

a) Re-Identification. With static de-identification, as long as any "utility", meaning implicit information, remains in the data there exists the possibility that some information might result in re-identification.

b) Lost Data Value. Generally, privacy protection improves as more aggressive static de-identification techniques are employed, but less utility remains in the resulting data set because static de-identification techniques remove identifying information from data.

c) Security Breach Exposure. The scope and frequency of data security breaches have changed the privacy paradigm. Some view theft of personal data by cybercriminals as the number one threat to privacy.[2] However, static de-identification techniques are not designed to improve data security.

d) International Acceptance. The decision this week by the European Court of Justice (ECJ) to invalidate the 15-year-old "Safe Harbor" agreement over concerns of non-compliance by U.S. companies with EU data protection laws, together with the EU General Data Protection Regulation (GDPR), recently passed by EU Parliament and due to become law by the end of 2015 (with penalties as high as five percent (5%) of global revenues for non-compliance), make it clear that compliance with U.S. domestic privacy laws by relying on click-through terms and conditions and/or static de-identification techniques may prove insufficient grounds to legally use data in other jurisdictions.

Existing technology does not effectively address shortcomings of static de-identification nor does it adequately reconcile conflicts between protecting personal data and enabling commerce. Because of this, companies can be placed in the uncomfortable position of choosing between delivering products and services to consumers or complying with data privacy laws in:

a) Jurisdictions that require unambiguous consent to use personal data like in the EU;

b) Industries subject to specific regulatory restrictions on data use like healthcare, education and finance in the United States; and

c) Other data use scenarios subject to uncertain future.

In a report submitted to President Obama in May 2014 entitled *Big Data and Privacy: A Technological Perspective*,[3] a working group of the President's Council of Advisors on Science and Technology (PCAST) noted:

[2] Robinson, Teri. "Privacy Matters." *SC Magazine*. May 1, 2015. http://www.scmagazine.com/privacy-matters/article/409041/

[3] https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

> *The beneficial uses of near-ubiquitous data collection are large, and they fuel an increasingly important set of economic activities. Taken together, these considerations suggest that a policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth).*
>
> *More broadly, PCAST believes that it is the use of data (including born-digital or born-analog data and the products of data fusion and analysis) that is the locus where consequences are produced. This locus is the technically most feasible place to protect privacy.* ***Technologies are emerging, both in the research community and in the commercial world, to describe privacy policies, to record the origins (provenance) of data, their access, and their further use by programs, including analytics, and to determine whether those uses conform to privacy policies. Some approaches are already in practical use.*** (emphasis added)

Dynamic Data Obscurity can help provide flexible technology-enforced controls necessary to support economic growth requiring sophisticated handling of various data privacy requirements. For example, the ability to deliver on the many promises of "health big data" is predicated on the ability to support differing privacy requirements depending on the source of health-related data:

- Consumer health data collected using personal health record tools, mobile health applications, and social networking sites are subject to privacy policies / terms and conditions of applicable websites, devices and applications;
- Protected health information (PHI) is subject to privacy and security requirements under the Health Insurance Portability and Accountability Act (HIPAA); and
- Health data from federally funded research is subject to separate privacy requirements of The Federal Policy for the Protection of Human Subjects or "Common Rule."

Each of the above categories of privacy and security requirements can be supported via Dynamic Data Obscurity despite differences in requirements – therefore opening up new opportunities for economic growth, and innovation in research and healthcare.

II. History of the term Dynamic Data Obscurity

One of the earliest mentions of the power of obscuring data was in a 2013 California Law Review article entitled *The Case for Online Obscurity*[4] by Woodrow Hartzog and Frederic Stutzman, in which they stated:

> *On the Internet, obscure information has a minimal risk of being discovered or understood by unintended recipients. Empirical research*

[4] http://www.californialawreview.org/wp-content/uploads/2014/10/01-HartzogStutzman.pdf

> *demonstrates that Internet users rely on obscurity perhaps more than anything else to protect their privacy. Yet, online obscurity has been largely ignored by courts and lawmakers. In this Article, we argue that obscurity is a critical component of online privacy, but it has not been embraced by courts and lawmakers because it has never been adequately defined or conceptualized.*

The term Dynamic Data Obscurity was coined in an October 15, 2014 blog by Martin Abrams, the Executive Director of the Information Accountability Foundation, which stated:

> *The fact is that we data protection professionals cannot accept the status quo. We need to be able to demonstrate our trustworthiness, and effective tools are part of that.*
>
> *The Information Accountability Foundation's mission is research and education on policy solutions that facilitate innovation while protecting individuals from inappropriate processing. As we have worked through big data ethics, it has reinforced our view that outside of the box technology solutions must be available. Data needs to be visible when it is being used within bounds, and obscured when it is not. Technology does not replace policy enforcement; it makes the enforcement possible and actionable.*
>
> *A number of us have been thinking about the dilemma for the past six months and looking for solutions. We believe the solutions are part of a field we have begun to call "Dynamic Data Obscurity." Dynamic data obscurity involves obscuring data down to the element level when that level of security is necessary and making sure that rules which control when elements can be seen are real and enforced. Dynamic data obscurity is also about making the technology controls harder to break but still allowing for appropriate uses. It requires both new technologies combined with effective internal monitoring and enforcement.*[5]

The next public use of the term Dynamic Data Obscurity took place in an October 20, 2014 International Association of Privacy Professionals (IAPP) Privacy Perspectives article[6] written by Gary LaFever, Co-Founder and Chief Executive Officer of Anonos - a pioneer in developing practical applications of Dynamic Data Obscurity technology, in which he stated:

> *We're not discounting the value of anonymization; it powered the growth of the Internet. But today, technology, markets, applications and threats have evolved while the protocols to keep personally identifiable data anonymous have not. If we are to mine the vast potential of data*

[5] http://informationaccountability.org/taking-accountability-controls-to-the-next-level-dynamic-data-obscurity/
[6] https://privacyassociation.org/news/a/what-anonymization-and-the-tsa-have-in-common/

analytics to create high-value products and services that improve and even save lives while meeting the privacy expectations of the public and regulators, we need new tools and thinking.

Dynamic data obscurity improves upon static anonymity by moving beyond protecting data at the data record level to enable data protection at the data element level. Dynamic data obscurity empowers privacy officers to improve the "optics" of data protection for data subjects, regulators and the news media while deploying next-generation technology solutions that deliver more effective data privacy controls while maximizing data value.

Vibrant and growing areas of economic activity—the "trust economy," life sciences research, personalized medicine/education, the Internet of Things, personalization of goods and services—are based on individuals trusting that their data is private, protected and used only for authorized purposes that bring them maximum value. This trust cannot be maintained using static anonymity. We must embrace new approaches like dynamic data obscurity to both maintain and earn trust and more effectively serve businesses, researchers, healthcare providers and anyone who relies on the integrity of data.

The Information Accountability Foundation held a framing discussion in January 2015 in Washington DC at which invited government, education and business leaders discussed that:

Early analytics, dating from the 1980s, were dependent on anonymization and de-identification to ensure compliance and individual protection. For example, information used for credit marketing needed to be de-identified to comply with the Federal Fair Credit Reporting Act. Technology provided the tools to de-identify, and the assurance came from the requirements of the FCRA. Effective de-identification and anonymization tools have always rested on this marriage of policy and technology.

Today's analytics, driven by observation, makes the mandate for the "belt and suspenders" of policy and technology even more compelling. The technologies are challenged internally by organizations' need for knowledge and externally by very smart cyber criminals. Even with the belt of policy, the suspenders of technology need upgrading to match today's challenges. If we do not meet that challenge, we could see real resistance to the information age's dual mandates for innovation and fairness. The policy community needs to explore Dynamic Data Obscurity

(DDO) to see if it will enhance data security and privacy to facilitate increased data value and protection compared to legacy approaches.[7]

The term Dynamic Data Obscurity has since been used at international conferences,[8] in comment letters submitted to international data privacy regulators,[9] and in White Papers[10] on the subject of Dynamic Data Obscurity.

My research includes a detailed analysis of the Anonos approach to implementing Dynamic Data Obscurity as well as coverage of issues generally applicable to Dynamic Data Obscurity – an important recent trend related to consumer privacy and data security.

I appreciate the opportunity to submit my research entitled ***Data privacy in an age of increasingly specific and publicly available data: An analysis of risk resulting from data treated using Anonos' Just-In-Time-Identity Dynamic Data Obscurity methodology*** to the Federal Trade Commission in connection with the FTC conference on January 14, 2016 regarding important recent trends related to consumer privacy and data security.

Respectfully Submitted,

Sean Clouston, PhD
Public Health
Health Sciences Center, #3-096,
Stony Brook University
Stony Brook, NY, 11794-8338

[7] http://informationaccountability.org/iaf-will-convene-ddo-discussion-in-2015/
[8] http://informationaccountability.org/video-of-panel-on-dynamic-data-obscurity/
[9] http://www.anonos.com/anonos-enabling-bigdata/
[10] http://www.anonos.com/anonos-dynamic-data-obscurity/