White House Office of Science and Technology Policy

Request for Information Regarding Data Portability

Public Responses

January 10, 2017

Respondent 1

Jay Wack, Tecsec Inc.

The enterprise attack surface continues to expand. Network borders are evaporating as data scatters across cloud, mobile, remote, and partner and other third-party environments. Multiple entry points into the network have appeared, prompting sophisticated data thieves to unite globally and create profitable data-theft businesses.

Thought leaders are aware of both the new risks and the role of data-centric encryption technologies in mitigating those risks. At the same time, however, many seem overwhelmed by the shifting security environment. Folks I have spoken to admit they haven't progressed sufficiently toward fully embracing data-level protection as a path to safeguarding data in its various states—at rest, in transit, and in use. Logically nearly everyone agrees but then hesitate because it requires "change".

The problem; sensitive data that is not protected and is in use by applications, analysts, business process users, and data scientists, is highly vulnerable to cyber-attack. Industry discussions have shown that data residing in an application or moving across a network is more vulnerable to external theft. And all data is repurposed.

Some reports indicate that more than 80% of data breaches happen at the application level. Container approaches, however, that don't account for the fact that data doesn't stay in one place. Gaps can crop up between protected data containers when data moves. In contrast, encrypting at the data level protects the data regardless of what state the data is in and where it is located.

Security risks and solutions have grown multidimensional, and new rules apply when data spills over corporate borders into the cloud and data lakes, and onto mobile networks and public Internet connections. Encrypting data at the data level keeps it safe regardless of what state it is in and where it moves.

Simply put, encrypting at the data level (which is more granular than a container approach) is a necessary key to protecting data at rest, in transit, and in use.

Jay Wack
Tecsec, Inc
XXX XXX XXXX

Respondent 2

Panha Chheng, Medyear

Commenting on topics #1 (benefits and drawbacks) and #3 (specific steps to take)

Hello, and thank you to the Obama Administration and the team at the OSTP for putting the issue of data portability at the forefront of our national policy conversation. I am Panha Chheng, the CEO of Medyear. I had the honor of working for President Obama during this 2008 election campaign (in Wisconsin) and know that we are in extraordinarily capable hands with our leadership in the White House.

Data portability is the future, and will embolden much needed progress across all sectors of our economy and civil society. In the world of healthcare, where Medyear operates, it can save lives, by ensuring that a medical history is complete and important life-saving information is readily available. It can also free our citizenry of "institutional lock-in," wherein people are forced to keep coming back to a given provider because that provider has a substantial portion of their health information. I believe data access and portability will enable our citizens to be more nimble and resilient, and our nation should be the global leader in this new frontier.

And yet, there is unfortunately a drawback – or rather, dark side - to the emerging frontier of data portability. This dark side is borne of an opportunism and greed that perniciously undermines the very aims of data portability in the first place. In short, people are beginning to realize that there is money to be made in data access and portability, and consequently will be looking for ways to line their pockets. Therefore, my following remarks are a sort of "manifesto" or rallying cry that I hope our leadership will embrace as we set out to cultivate a new frontier of responsible data access and portability.

The apt metaphor is the "toll road" in which organizations can monetize the portability of data. Generally, toll roads are beneficial for society as they allow certain routes to be completed much more quickly. However, when those toll roads lack accountability or are poorly managed, the human penchant for greed or lust for power may take over. And when that happens, those organizations could harm both the lives of American citizens and the public trust.

Medyear actually helped build one such "toll road" for a publicly-funded state health information exchange recently. In fact, we even won a federal government award for it, as part of the ONC's health data aggregator challenge. At the onset, things were looking pretty good. We had a compelling user experience built especially for patients in the state, and the state exchange had built considerable data connectivity across 67 entities throughout.

The "toll road" we helped build enabled the digital delivery of an immunization history and forecast from a state registry to Medyear's mobile application. It was designed for parents to use when getting their kids ready for school or summer camp. In theory, it would save the parents from having to take a day off of work to make the trip to the doctor for the paper record. And for such a nice convenience, parents would pay a reasonable amount. Pretty groundbreaking, if you ask us.

Then, this project took a turn for the worse. The details are messy and inappropriate for this forum, but after building the necessary translation tools for data passing to and from the state immunization registry the project hit a roadblock when the we tried to clarify the real-world scenarios for the end user accessing information from their smartphone. Because of disagreement on how the data that patients pay for might be stored, we were concerned that there was a "pay to peek" scenario emerging.

Offering patients only a glimpse at their data stands in stark contrast to the clear pronouncements from the HHS Office of Civil Rights regarding a patient's right under HIPAA to obtain a copy of their health information and use it in any way they see fit. So, as patient advocates hoping to see patients have as much meaningful control over their data as possible, we voiced concerns about a patient's right to access as governed by HIPAA. In response, the state exchange took the action to sever its partnership with Medyear.

This was disappointing, and not being in the state certainly hurts our business, but such actions are common given the human penchant for greed. Therefore, Medyear believes such "toll roads" will need considerable oversight if they are to function properly and work in the best interests of the citizenry. With appropriate oversight, and beneficial tools like Medyear in the hands of our nation's patients, our citizens can stay healthy and our society can be uplifted by technology. Transparency and discourse about business models and best practices will go a long way, but we must be on the lookout for the new greed that comes with exploiting data portability frontiers and defeat it before it undermines data access in the first place.

In terms of specific recommendations, Medyear hopes that the Obama Administration will embolden the HHS Office of Civil Rights to take action against cases of abuse, and make examples of bad actors. In cases of abuse or mismanagement at publicly-funded entities, we should have the GAO engaged in reviewing and auditing the practices of these publicly-funded entities that are monetizing off of data access and portability. Such entities should be prohibited from implementing "pay to peek" schemes that undermine a patient's ability to have potentially life-saving at their fingertips.

The President should also speak to the American people directly about their rights and how their government supports those rights. I would encourage President Obama to hold a townhall on the topic, and guide landmark legislation through Congress that would govern the new frontier of data access and portability. In such legislation, it would be prudent for old data standards to be updated, public organizations providing access to have considerable oversight, and private companies providing data access and portability to adopt a sufficient level of security controls to ensure the public safety.

Finally, special attention must be paid to the use of data handled by an artificial intelligence. A.I.s do not currently possess human morality and sensibilities, but yet could someday have domain over a human's data, or domain over how a human uses his or her own data. This introduces a complex array of ethical questions and potential risks. Therefore, the Administration should rally a commission of our nation's leading bioethicists and data scientists, whose charge is to ask tough questions about an A.I.'s role in data sharing, and promulgate recommendations for how to govern the productive participation of non-human actors in a data ecosystem.

Someday, with the right data governance policies in place and a thriving ecosystem of innovators, an A.I. could very well help realize the President's vision for Precision Medicine and the Cancer Moonshot. For this to happen, patients need to be able to access and share their data seamlessly across institutional and state lines. Medyear embraces this bold vision. We represent a growing group of innovators that seek to help consumers take control of their health information, so that they can lead healthier lives and when they get sick, be cured of their disease.

This administration has done incredible work to release health information such that it can be put to use to improve our nation's health. The old ways, where data was locked away in proprietary silos, have failed us. Thankfully, we now have a new paradigm in which a patient manages his or her own medical records. As this new paradigm is established, it is critical that federal and state organizations establish ground rules to ensure there is fairness and transparency within the new economic landscape of data liquidity. Better yet, if the government leads by example, this will go a very long way towards ensuring that data can flow in meaningful ways and uplift lives.

I would be honored to participate in any government action in support of such a mission and would readily lend my expertise where needed. And as one of the world's first consumer-mediated health exchanges, we would also be happy to contribute our experiences in the dialogue around data portability best practices. The fight for a patient's civil rights continues. We are honored to be at the frontier.

Panha Chheng
CEO, Medyear

Respondent 3

Brian Weiss, Carebox Healthcare Solutions, Inc.

(1) the potential benefits and drawbacks of increased data portability

It is rather frustrating that it is still considered a public policy "question" whether patients should have the right to access and share their own data. HIPAA regulations and OCR policy have been very clear (and recently, I've been pleased to see, getting more clearly re-enforced at the messaging level) on this point.

It's impossible in my mind to separate the question of "healthcare data portability" from the question of "patient healthcare data access". So, it's puzzling to me that anyone would think that obstructing a patient's access to their own healthcare data due to "drawbacks of increased data portability" is a legitimate position for the US Government to consider.

I also was disappointed to see it stated here that "perhaps the most important benefits are the ability to create backups". The most important benefit to patients are the ability to stay alive and to be healthy. OpenNotes has featured compelling stories like this one: https://www.youtube.com/watch?v=Glo5zP3sMpM

Whether patient access and control of their own healthcare data has benefits or not (and it has many, as I will note in the next item response), the notion that we would allow healthcare service providers to lock up a patient's healthcare data and lock-in patients for any reason, should be untenable in any case. The counter-arguments presented here sound like blackmail demands by healthcare providers and their vendors. I suppose by that logic, healthcare providers should be exempt from any rules and laws of our society intended to benefit all… otherwise they "might adjust their business models and become more selective in their initial customer acquisition strategy or invest less in their customer relationships".

(2) the industries or types of data that would most benefit or be harmed by increased data portability

I believe it is well understood by many (including leaders past and present at HHS/ONC) that the benefits of data portability are critical to enabling any substantial transformation in continuity of care, value-based payment reform, and other fundamental aspects of the cost and quality of US healthcare. Those translate directly and unequivocally into the health and well-being of the US population.

Data portability under patient control/consent would also transform clinical research and clinical trials, is key to precision/personalized medicine, key to patient-centric health services, and would usher in a new era of healthcare analytics and applications – from medication adherence and safety to chronic care management, to health and wellness solutions.

Yes, it also enables anyone to backup their data. And share it. And do anything else they want with it. Indeed, most of the use-cases and benefits that will evolve once data portability has been enabled have not even been dreamed up yet.

(3) the specific steps the Federal Government, private companies, associations, or others might take to encourage or require greater data portability (and the important benefits or drawbacks of each approach);

Most of what is needed is enforcement of the already stated policies as per https://www.healthit.gov/patients-families/accessing-your-health-information and the underlying HIPAA regulations and OCR clarifications it represents. Any healthcare service provider that doesn't make it easy, free, and instantaneous for any requesting patient to get their electronic information in available or reasonably achievable formats – should be prosecuted and penalized in way that ends the current farce whereby it's a "legitimate business decision" for them to decide if they feel like obeying the law or not.

Exactly as laid out on the healthit.gov website noted above, this has to include ALL information – not just a CCD with the "core data set" of Meaningful Use. All pathology and radiology reports, all doctor notes. Everything. If a doctor can see it on a computer screen, so can a patient. If the hospital's internal IT department can get at it as structured data for analysis and reporting – so can a patient. That is the simple litmus test.

(4) best practices in implementing data portability;

Data portability exists today in a primitive form. Armed with several hundred to several thousand dollars, four to eight weeks of patience, and several hours of personal investment above beyond that being paid for to a specialist service provider, anyone can get most of their medical records and "port" them wherever they want.

Transforming that current state of affairs into what the letter and spirit of the law currently requires is all that is needed. We don't need public policy to dictate technology standards. Private industry can and will sort out the rest.

For example, if patient portals (or any conceptual equivalent) were universally required and were enhanced to include any data and document that is available internally to the healthcare service provider (as per the litmus test noted above) – that would solve over 80% of the challenges that exist today.

(5) any additional information related to data portability policy making, not requested above, that you believe OSTP should consider with respect to data portability.

Two additional thoughts…

A) We need to limit the privacy/trust/authentication/security "excuse" to block patient access to their own health data. Just like a patient can securely log into a patient portal (or financial institution, travel site, social network, etc.) using a user name and password they receive online, they should be able to "log in" via any application of their choosing using the same credentials.

There are legitimate privacy/trust/authentication/security concerns when it comes to healthcare data but the risks associated with patient-centric data portability are highly inflated. Most breaches (large insurance databases, credit card data), document leaks, ransomware, etc. are taking place irrespective of patient access.

If you give someone something they have a right to have, there is a chance it will fall into the wrong hands, or that they will put it in a place that is not safe. Consumers today can scan all their paper records and do whatever they want with them online. The same for any other sensitive information. Market dynamics will establish the correct trade-offs of ease-of-use vs. security/privacy as they do in all industries with online data elements (which is pretty much everything these days). I'm not convinced that the vast majority of consumers need more protection of their health records than of their emails, photos, hotel reservations, credit card statements, or anything else. But even if they do, that is not a reason to prevent patients from accessing their own data.

B) I would welcome the opportunity to walk OSTP through the ten pilot projects that I am involved with today with leading disease-specific patient advocacy groups, patient-powered research organizations, veterans care programs, pharma-sponsored genomic research, clinical trial recruitment, life insurance underwriting, and more. These are incredibly compelling today – despite the fact that practical patient-authorized medical record collection is made nearly impossible by healthcare service providers. Even modest improvements in data portability via enforcement of existing laws and policies, as outlined

above, would be incredibly transformative and, I believe, render the need to "debate the benefits and drawbacks" as silly (to be kind) as it really is.

Respondent 4

David Nuss, Self/Consumer

Thanks for studying this. I am backing away from proprietary services of many kinds in order to protect MY data.

(1) the potential benefits and drawbacks of increased data portability

Benefits to consumers are manyfold and obvious, you know that already. Drawbacks are that companies that perpetuate hardware and software silos will lobby gov't against portability and gov't will have to stand up to that for The People.

(2) the industries or types of data that would most benefit or be harmed by increased data portability; photos, documents, passwords and notes in password management software, twitter history, instagram and other social media posting histories would all benefit. I don't really see a media type that would be harmed.

(3) the specific steps the Federal Government, private companies, associations, or others might take to encourage or require greater data portability (and the important benefits or drawbacks of each approach)

Well, Feds: find out what Europe does, they are generally more advanced than we are on privacy and data protection; harmonize with the world standard on this as a starting point. Companies need to figure out a mutually beneficial means for customer data portability. They need not fear it if it's done right. Associations can set standards, ie what are the data portability file formats that need to be kept alive and set up non profits with corp and gov support to maintain those formats and/or provide translation tools to future formats, when companies abandon those formats.

(4) best practices in implementing data portability; International standards.!!!

(5) any additional information related to data portability policy making companies from FB to Apple and MS and others are luring users in with products and adding features that lock customers into their silos. so their business model is fear... of losing data, connections to family/friends/business associates etc.

Gov't needs to work with non profits and int'l bodies to keep companies from doing this. Help promote RSS and self-hosting/easy hosting and subscription to give users both the convenience of FB and twitter as well as the ease of use. look at what Indieweb is doing.

Good luck and may you be successful!

Respondent 5

Drew Mingl, State of Utah

The health All Payer Claims Database (APCD) contains claims data from health care payers/providers. They are designed to inform cost containment and healthcare. Many states CHARGE to access these data which defeats the entire purpose of collecting it. Free and open this data. #opendata

Respondent 6

Kady Hill, Arkansas Heart Hospital & Clinic

In our case, our ambulatory vendor decides what information we can publish electronically to our patients & there has been no enhancements since buying this product in 2012. I've even had discussions with the CEO & COO explaining the importance of this. Our hospital vendor lets us decide what info to give patients access to. We do not restrict any reports, results, or patient documents. Full transparency. Why are EMR vendors not scrutinized by the ONC? Why should by organization be restricted by my ambulatory EMR? The ONC needs to see real versions of the software in use - not just test versions & specs provided by vendors. As an informatics nurse it also frustrates me that there are still so few practices using a portal. My child's pediatrician is a perfect example. I wait 3-5 business days for an immunization record. This is 2016. Same thing with my PCP. No portals, no visit summaries. My elderly parents get Visit summaries....ones that are blank and provide zero value to assist me in managing their healthcare. It's time to quit checking boxes to avoid penalties & actually give patients useful data. Hold EMR vendors accountable

Respondent 7

Amy Robison, SEED Protocol LLC

2. All industries could benefit from increased data portability, provided it is secure. However, the healthcare industry and its patients (All of us!) have the most to gain from increased data portability because it is absolutely vital for coordination and continuity of care, not to mention efficiency. Many patient engagement and advocacy groups are calling for patient-centered health records. We agree this is the best path forward. People want access to and control of their health data; they should have it.

4. We believe the Secure Exchange of Encrypted Data (SEED) Protocol should be the standard for secure data portability. The SEED Protocol is a patented solution (U.S. Patent Nos. 9,378,380 and 9,390,228) that combines individualized, asymmetric encryption with a distributed, interlocking design. Three computing systems work together to keep confidential information safe; hacking any one of the systems does NOT compromise protected data.

For brief, accessible videos explaining the SEED Protocol and more detailed information on the technology behind it, please visit: https://www.seed-protocol.com/press/",
"Organization": "SEED Protocol LLC

Respondent 8

Steve Boms, Evestnet Yodlee

Envestnet | Yodlee ("Yodlee"), the leading global account aggregation platform provider, appreciates the opportunity to provide comments to the White House Office of Science and Technology Policy ("OSTP") in response to its request for information regarding data portability. Yodlee, which is supervised by the Office of the Comptroller of the Currency, provides consumer-permissioned account aggregation capabilities on a business-to-business basis to consumers around the world, which include some of the nation's largest banks and leading financial technology companies. Our clients offer data from Yodlee's platform to millions of retail consumers through financial wellness solutions, which provide a single platform for consumers to track and manage their financial accounts at different banks and financial institutions with a consolidated financial viewpoint. Yodlee clients can also use Yodlee's platform to verify consumers' access to their account in real time and for risk management purposes.

Yodlee's client base includes 12 of the 20 largest banks in the United States and the largest global banks in more than 20 countries. Yodlee also acts as a critical technology partner that enables the growth of the FinTech marketplace by supporting many well-known companies that are innovating within the financial services sector.

Yodlee is pleased to have the opportunity to offer the following comments in response to OSTP's request for information, with a particular focus on question 1, which asks about the benefits of increased data portability, and question 3, the specific steps needed to encourage greater data portability. Consumers' access to, and their right to share this data with, providers that can help them achieve their financial outcomes, is fundamentally a data portability issue.

According to the Federal Reserve's 2016 survey on Americans' economic well-being, one-third of Americans are struggling financially and 42% of Americans were unable to pay their bills at least one month within the last year. Nearly half of American households would have to incur debt or sell assets to pay for a surprise $400 expense. The only sustainable path toward improving Americans' financial lives is one that allows Americans to access their financial information via the tools and providers they choose to help them improve their financial health.

Consistently reliable access to real-time, up-to-date and accurate banking and other financial transaction-level information – credit and debit card transactions, investments and

loans, for example – is an incredibly valuable tool and enables consumers to improve their financial state. By allowing consumers to permission electronic access to their financial transaction data by responsible service providers, American consumers can utilize a vast suite of solutions and advisory services specifically designed to improve consumer financial wellness. These tools cover a wide range of needs, from simple budgeting programs, to optimizing fixed incomes, to informing sophisticated investment management tools. In addition, these tools support consumer objectives of evaluating the benefits of the financial products they qualify for, avoiding attempts to spend money that they do not have, and escaping incurring late fees or penalties or the need to entangle themselves in predatory loan products.

However, recently Americans' access to their financial transaction data to power these helpful tools has become more problematic. Some U.S. financial institutions have instituted a range of technical and administrative hurdles that interfere with the consumers' rights of access and portability of their data. Financial institutions have moved to limit the amount of data that consumers can share, or are seeking to define bilateral agreements with onerous contractual terms that would restrict consumers' ability to take full advantage of marketplace solutions that would empower them to make better financial decisions. These institutions are able to make this interference because the existing statutory and regulatory environment in the United States does not clearly provide consumers a guaranteed right to electronically access and share their personal financial transaction information. As a result, there are an escalating number of cases where consumers are excluded from engaging with services provided by the financial technology community best suited to improve their financial wellbeing.

To remedy this situation, Yodlee proposes the creation of a Consumer Bill of Data Rights that codifies a consumer's absolute right to control access to, and portability of, their own financial transaction data and, in turn, to utilize the power of technology to improve their financial wellbeing. These rights must be granted in a balanced principled ecosystem that should also define the consumer's role and obligations. These include the responsibility to make informed decisions, follow reasonable practices, participate in awareness and education activities and otherwise engage with their service providers and data sources as reasonably requested; as well as standards and guidelines for FinTech providers, data aggregators, and the financial institutions hosting the data.

A core role in this newly balanced ecosystem rests with the data sources themselves, such as financial institutions. Fundamentally, data portability requires unfettered access. For this reason, Yodlee also proposes that data sources should be required to allow a consumer to access their data directly, at any time, or to provide permission for a qualified service provider or aggregator to do so on their behalf. This access should be available via a standard API, batch file and/or screen scraping so that smaller data sources, like community financial institution, are not unduly burdened with the cost of implementing and maintaining an API, thus excluding them and their customers from the benefits of this

balanced ecosystem.

Realizing the full potential of financial transaction data access and portability – the democratization of data – comes with requirements for all stakeholders in the 21st century's financial services system, all in support of enabling and protecting the American consumer and their financial data. The growth of the financial technology sector brings with it immense opportunities to empower Americans to take better control of their finances, and, in turn, to offer their children the essence of the American dream: a life better than their own. Yodlee fully supports the OSTP in its initiative to understand the opportunities and challenges of consumer-permissioned financial transaction data portability to fulfill this promise, and is pleased to offer our expertise and experience.

Respondent 9

Owen Mundy, Davidson College

Hello,

Thank you for the opportunity to contribute to an understanding on data portability. I am the author of Give Me My Data which provided ways for regular users to export their data back *out* of Facebook in reusable formats. While the attention my app received influenced Facebook to create their own method for allowing users to get their data out, Facebook does not allow the data to be exported in formats that are easily reused. Alas, Facebook eventually changed their policies and denied my app the possibility to request permissions to access user data thus forcing me to shut down. The statement is here http://givememydata.com/ Walled gardens like Facebook, which have evolved to depend on legal surveillance of user data to sell advertisements, will always resist measures to allow users control over their data. These companies see it as a commodity, ignoring the rights people should have. A greater change in privacy laws which give people more rights, similar to those in Europe, are needed before data portability can adequately be improved. There is much more to say on the subject so feel free to contact me after reading the statement at the link above. Best, Owen Mundy

They will only work for their own survival, dominance and propagation. Our own AI programs are routinely mopping the floor with our best fighter pilots in test scenarios. Thats some incredibly advanced programming right there. Then imagine that machine understanding how it can be turned off at a moments notice and not wanting that to happen. Our goose will be cooked. If AI leads to sentience, we are, to put it quiet simply, screwed.

Respondent 10

Ben Newton, audriga

Bottom Line: Data portability is a net win-win for businesses and consumers. Government should engage with businesses and consumers to facilitate this realisation. A different strategy may be necessary as the situation develops. The potential downside of premature government action could be catastrophic, and not easily reversible, as flight to another legal and tax regime is, over time, increasingly reduced to mouse clicks, leading to a potential Data Exodus. Additionally, premature government action could be interpreted as part of a larger trend away from the rule of law, at least at the perception, if not necessarily the fact level. Other legal regimes, particularly the EU, could serve as a test bed for both business and government responses.

It is my strong opinion that this strategy will preserve the greatest possible freedom of action for the longest time into the future.

(1) the potential benefits and drawbacks of increased data portability;

Highly influential market leaders are both aware of and front running data portability, which I believe is already an emerging standard. I have seen evidence of this in my professional work dealing with email migration. While there is some disagreement amongst my colleagues as to how deeply this realisation has penetrated the wider industries we touch, I believe the net flow of customers, and their attendant revenues, will, over time, increasingly tilt toward toward businesses embracing data portability as customers assert their interests with their wallets.

Generally, businesses will see more profit over time as they embrace a larger revenue pie with higher risk of customer outflow, and therefore less revenue per customer. They will realise that the tradeoff between locking in customers, and data portability comes down to nothing more than a different way of modelling time, profit and revenue per customer, with data portability generally resulting in more money over time.

Technical convergence may in the end be the strongest factor, far stronger than the above economic win-win scenario, potentially turning it into something more like the rationalization of a self fulfilling prophecy. However, the likelihood and dynamics of that sort of widespread technical convergence are difficult to predict, and no argument against the merits of the above win-win scenario.

Technical convergence also calls into play Gödel's First Incompleteness Theorem, which in its shortest and most germane formulation says: no algorithmic system can be both consistent and complete. In plain terms, this means technical convergence cannot, as a matter of necessity, account for the whole of any reasonably large real world problem without being a continuously adjusting dynamic, which itself cannot be controlled by an algorithmic system. Examples of real long lived systems which defeat Gödel are: in the world of human affairs, the whole of the scientific process, writ large; and in the natural world, Natural Selection, particularly in its penultimate description, Punctuated Equilibrium.

All Black Swan Events are caused by Gödel, or some of his second/third order effects, as far as I'm concerned. However, I believe I'm an outlier in this regard.

With regard to potential security risks, I highly recommend engaging the ODNI on this topic, preferably at the classified level. Based on my experience as an intelligence officer in the US

Army, with regard to the intelligence community, data portability, particularly as an outgrowth of data interoperability, is a problem which has been solved, the solution implemented, and while the resulting ecosystem is still evolving, I would call it mature. There are clear security versus portability/interoperability tradeoffs, in my experience, but I believe it all comes down to one's degree of confidence in a strategy of security through obscurity versus one's confidence in their own ability effect real world outcomes.

(2) the industries or types of data that would most benefit or be harmed by increased data portability

Alexander Macgillivray mentioned two types of second/third order data in Exploring Data Portability, (https://www.whitehouse.gov/blog/2016/09/30/exploring-data-portability) data collected about the user, such as usage data, or even conclusions drawn by the service about the user. If these types of data are forcibly released it will cause catastrophic real world business consequences. Any new business predicated on these types of data would be untenable in such a legal regime, and must necessarily be founded outside of the United States. Any existing business would have to flee, or go bankrupt.

However, it's not as simple as more business, good, less business, bad, which is a reductive and absurd way to view the intersection of commerce, common sense and good government policy. It may be that some businesses ought not be around, ones using force and fraud for example. I think one of the key outcomes of letting the situation unfold a bit is that there will likely be some degree of clarity as to the desirability, classification and identifiability of emerging real world business outcomes.

I suspect the first class he mentions, data collected about the user, such as usage data, will provide the basis for businesses which are identifiably distinct from businesses predicated on the second type, conclusions drawn by the service about the user, and have distinct second/third order effects. I think businesses based on the first type of data are much less systemically important for two reasons: this sort of data is generally boring and well trodden, based on my time as a product manager at a data marketplace startup; they have been around for a long time already (spammers, but also targeted, relevant and desirable advertising for example), creating a relatively secure, and boring place in the ecosystem; and, I strongly suspect they will be disrupted as consumers continue to drive data portability. I don't think a future with some flavor of personal data cloud and personal APIs to be all that strange, or even far off. (I've encountered multiple entrepreneurs working in this sphere.) That future may present its own problems, however.

Business predicated on the second class of data will also flee if there is any meaningful likelihood of there data being forcibly released. I believe this is a more serious and systemic economic threat, as this sort of data, what I see as truly valuable metadata, is and will be the basis for much economic value, I think it highly likely that it will be the majority of future economic growth in any highly advanced economy.

Businesses are already fleeing in different, but perceptionally related areas, and I assert this would serve as a prologue for a potential Data Exodus.

Possible leading indicators of the Data Exodus :

Microsoft has set up a wholly German cloud in order to allow customers to escape second/third order post Snowden effects.

I used to be the CEO of a white label Bitcoin software exchange company (Mimetic Markets, Inc.), and while we were an American company, we did not do business in the US, due to uncertain regulation and enforcement, which posed a direct and existential threat.

Ethereum, an interesting blockchain startup (nearly $1B market cap!) had to be founded in Switzerland for much the same reasons.

Other information regarding costs and benefits:

To some extent, commodity services like cloud-based email already offer a certain degree of data portability by means of established APIs/standards (e.g., IMAP) and those industries show some healthy competition.

Conversely, novel services, e.g., in online healthcare etc. lack established standards while they could perhaps benefit most from allowing for data portability. However, innovative services often predate standardization. So this perhaps one of the issues most difficult to overcome in data portability in general.

Note that Apple iCloud does not offer any means/APIs beyond some Apple tools (iTunes) to access iCloud stored photos/files. This is a very notable but relevant example.

Another notable example is LinkedIn, which once offered APIs to easily access one's data. However, that API access was subsequently removed, such that there is no easy way to get one's data out in a structured format nowadays.

(3) the specific steps the Federal Government, private companies, associations, or others might take to encourage or require greater data portability (and the important benefits or drawbacks of each approach)

Step one: cast the net widely and publicly when it comes to talking about this topic. (As an officer, I've found the Army's intellectual culture of open and vigorous debate generally yields a 60% solution without top down direction, simply by virtue of intellectual convergence. Secondarily, when the debate becomes the grist for the decision mill, it enables well founded outcomes, both morally and materially.)

Step two: React to real world events, potentially, but not necessarily, with regulation.

In the future, there may be a role for government to hold bad actors accountable when they don't adhere to the industry standards which will emerge, or even to kill certain methods of business. However, I think using government force to enforce regulations which are premature, and therefore almost certainly as arbitrary as a broken clock, could have potentially disastrous consequences.

(4) best practices in implementing data portability

Google Takeout is often cited as a major practical example. While it deserves some first-mover credit, several things are notable here:

Google Takout comes as one single large dumped file, with subfolders per service (Mail, Drive, Contacts, ...). Some dumps are mere HTML or JSON files which are difficult to handle for end users. Also, mails are contained in an MBOX file, which is some de facto standard for storing mails. However, also this format is difficult to handle for the normal user (esp. labels/folder structure of mails).

Even a kind of standardized format like vCard, which is used for exported contacts, in practice has often vendor-specific extensions, which makes it unlikely to be portable somewhere else 1:1 without any data loss

Besides Takout, some Google services (e.g., Mail) can be accessed by standard APIs (IMAP in case of Mail). In practice, IMAP is the preferred way our company is use to onboard/offboard customer email from Google. This especially allows for direct end-to-end portability (copy directly from Gmail to Yahoo), without requiring the user to download/upload.

While APIs can thus play a vital role for data portability, their use is often restricted. E.g., Google has some not clearly documented throttling limits on its Gmail API and other APIs

Note that in the email cases, although IMAP is an established de-facto standard, some vendors/plans might not offer IMAP access and thus inhibit data portability. Examples are Amazon WorkMail (IMAP in preparation), GoDaddy (some of their plans) or some freemail/cable providers; the latter only offering POP3 access, which does usually only allow access to Inbox emails.

Regarding APIs also note that many APIs so far are not designed for data portabilty . E.g., many online file storage services might not expose certain metadata (such as tags) via APIs. Interestingly, also onboarding APIs (for data portability TO another provider) often lack features - in the case of online file storage services e.g. the possiblity to set a different file time stamp than the upload date (i.e., uploaded files often show the migration time as their date - even for old photos etc).

(5) additional information related to data portability policy making

One last thing about the virtue of letting the situation develop: the EU has already legislated some form of data portability, so it might be useful to see what that experiment yields before committing to something. The big caveat is that the European context, culturally, historically, politically and legally, is very, very different than the context in the United States. For example, the 20th century experience with facist denouncement and Communist spying looms far larger than most Americans would be willing to believe. The original impetuous for the EU data portability paragraph was the relative power of Facebook as a social network. Few, if any, Americans would think all the cool kids being on Facebook requires a legislative response, for fear of being seen to not know about Instagram or Snapchat, being called an old foggy, and potentially reaching the Series of Tubes level on YouTube.

The different contexts at play in Europe will likely cut another way, however, in that there may be different, but desirable, future outcomes possible in Europe, and copyable in the United States.

Primary Author

Ben Newton

Director of Services

audriga GmbH (cloud, primarily email migration)

Durlacher Allee 47, 76131 Karlsruhe

Civil Affairs Team Leader (Reserves)

D CO 457th Civil Affairs Battalion

Grafenwöhr, Germany

Formerly:

CEO - Mimetic Markets, Inc. (white label Bitcoin exchange software company)

Product Manager - dmi.io (data marketplace)

Lead Kestrel Analyst - Wisdom Tree technologies (Intelligence Analyst in Sangin, Afghanistan)

Intelligence Officer - US Army

Infantryman - US Army (Advisor to the Iraqi Army, Bradley Commander)

BS Physics - Colorado State University

MA (ABT) European History, History of Science/Technology - University of Colorado Denver

Secondary Author

Hans-Jörg Happel

Cofounder, Managing Director

audriga GmbH

Durlacher Allee 47, 76131 Karlsruhe
dfssdf

Respondent 11

David Kibbe, Direct Trust

As President and CEO of DifrectTrust.org, Inc. (DirectTrust), a large, inclusive, and diverse health IT industry alliance non-profit, I would like to comment progress made to date in providing personal health information portability between providers of care, and between providers of care and their patients and consumers. Direct exchange is a secure transport methodology that is content neutral, such that files of any format may be attached and transported securely. This includes the most common structured data set for clinical health information, the C-CDA. But Direct exchange can and would be useful in transporting other structured data types for patients and consumers wishing to move their data from one area of storage to another.

First, let me comment on the state of adoption of Direct and its significant development as a standard for secure and interoperable health information exchange. The advanced stage of adoption reported on here is in large part a result of the early support that DirectTrust received as the recipient of a Cooperative Agreement with, and funding from, ONC under the "Exemplar Health Information Exchange Governance Entities Program" between 2013-2015. The primary mandate charged to DirectTrust by ONC under the agreement was the establishment of a large "trust community" that would build national scale for the trust relationships needed for provider and patient confidence in sharing of protected health information (PHI), making these data sets portable, such that individual parties to the exchanges would not need to engage in expensive and time-consuming one-to-one negotiations or agreements regarding policy and controls for privacy, security, and trust in identity, but, instead, would rely upon assurance resting on a common framework of technical standards, trust policies, and best practice requirements, voluntarily agreed to and enforced through: robust accreditation and audit of service providers; a brief legal agreement known as the Federated Services Agreement; and oversight by DirectTrust, its Committees and Board of Directors. I feel it is important to note the success of this governmental-private sector partnership as the foundation of current progress.

As of the second quarter of 2016, there are 40 DirectTrust accredited HISPs and 15 RA/CAs who together provide Direct messaging services to approximately 300 ONC-certified EHR technology companies and their customers. One of these HISPs is operated by the Veterans Health Administration, and another by the Indian Health Service. Some HISPs are operated as stand-alone service organizations, others as divisions of EHR and PHR vendors, others by HIEs, and still others by health care provider organizations. HISPs also provide Direct services to over 30 HIEs and their members, and to approximately 25 mHealth, PHR, and social website application providers and their customers.

DirectTrust member Health Information Service Providers (HISPs) have contracted as Business Associates to provide Direct exchange services with almost 60,000 health care

organizational subscribers, mostly hospitals, clinics, and medical practices, and also with an increasing number of long term post acute care, home health, and other ancillary non-EHR using entities. HISPs have become dynamic facilitators of interoperability for a wide range of customers, able to interface with virtually any edge system, and affordably connecting with many legacy health IT applications to provide real time interoperability for the first time.

Thus, data portability of health information is already at an advanced stage of development within the US healthcare system. This development is ready for much wider use by patients and consumers, as it is secure and ID proofed in a manner that meets federal standards for security controls. I would be glad to discuss this journey of over 5 years with you further. Respectfully, David C. Kibbe, MD MBA, President and CEO of DirectTrust and Senior Advisor, American Academy of Family Physicians.

Respondent 12

Linda Van Horn, iShare Medical

U.S. Office of Science and Technology Policy (OSTP)

Executive Office of the President

Eisenhower Executive Office Building

1650 Pennsylvania Avenue

Washington, DC 20504

Re: Request for Information Regarding Data Portability

To Whom It May Concern:

Thank you for the opportunity to respond to the Request for Information Regarding Data Portability. iShare Medical is one of 40 EHNAC Accredited DirectTrust Anchor Health Information Services Providers (HISPs) in the United States who facilitate the exchange of medical records in the healthcare industry. DirectTrust is a 501C (3) nonprofit created by a grant from the Office of National Coordinator for Health Care Reform. DirectTrust focuses on the data portability or exchange of medical records in the healthcare industry. This includes the bidirectional change of health information between healthcare providers and between providers and patients / consumers.

iShare Medical is the only EHNAC Accredited DirectTrust Anchor HISP that is also a National Association for Trusted Exchange (NATE) Trust Anchor for the NATE Blue Button for Consumers. NATE is a 501C (3) nonprofit created by a grant from the Office of National Coordinator for Health Care Reform. NATE focuses on the data portability or exchange of health information between providers and consumers.

Health data portability or information exchange is about it in the right information, on the right patient, to the right provider, at the right time, every time.

There are three main components of health data portability or information exchange, they are:

1. Identify proofing the individual or organization so that we can trust to whom we are exchanging data such as a physician, medical practice, or patient (e.g. end point)

2. Assigning a certificate or token that can only be used by the identity proofed individual or corporation that is used like a key to unlock encrypted messages

3. Data encryption and transportation of information\tbetween identify proofed authorized and trusted end points

Under HIPAA, patients / consumers have a right to their medical information and healthcare providers who are treating a patient have the right to information so that they can effectively treat the patient. But far too often, medical data is not available to the patient or their provider. In short, healthcare providers fly blind.

In a study published by researchers lead by Martin Markey, MD, MPH at John Hopkins, states that the third leading cause of death in the United States is preventable medical errors ; ranking just behind heart disease and cancer.

In short, access to medical information saves lives.

What if the doctor only knew the patient health history, drug interactions, genetics …? Perhaps we could reduce or eliminate preventable errors saving an estimated 250,000 Americans each year.

In addition, when providers do not have access to medical data they often order repeat procedures and diagnostic tests which drive up the cost of healthcare.

In short, access to medical information saves money.

We, at iShare Medical believe:

1. Patients and their providers need access to the complete medical record; one that is available in both machine readable and human formats

2. That medical records need to adhere to standard structured format with defined terminology so that they can be ready and understood by other systems

3. Patients, providers, and others authorized under HIPAA should be ID Proofed and assigned a credential that uniquely identifies them in the system. This credential eliminated the patient matching algorithms which at best are in the mid-80% reliable for a correct patient match .

4. Exchange should be encrypted and secure in accordance with HIPAA Security and Privacy Rules

5. There is a fiduciary obligation of the record holder to hold these records safe and secure.

6. Patients have the right to view, download, print, and otherwise obtain access to their data and that once the data leaves the record holders system that the record holder fiduciary obligation ends.

As a software vendor who focuses on health information exchange or data portability, we know firsthand that the healthcare portability is far from perfect today. Many providers block the sharing of data, use non-standard formats, or exchange data that is not machine readable. This only drives up the cost of healthcare, creates safety risks for patients and increases the likelihood of patient death by preventable causes.

Thank you for the opportunity to share our thoughts on the very important issue. Should you have any questions or need additional information, I can be reached at [REDACTED] or via email at [REDACTED].

Sincerely,

Linda Van Horn, MBA

Respondent 13

Brian Willard, Myself

I am excited that the OSTP is investigating data portability. In my experience this is often a feature users never look for when starting to use a service but always look for when they stop. Any efforts to raise awareness of the importance of portability within the industry and within public awareness will be a good thing.

These comments come from my experience running a large scale data portability program focused on consumer users for an internet company. They are aimed at sharing some concrete actionable suggestions.

(topic order is swapped but noted by (#))

(2) the industries or types of data that would most benefit or be harmed by increased data portability:

These comments are focused on consumer services, that are in general, provided for free. In these types of services user trade their data, and attention, for the services provided. In these cases their data is often the only leverage they have with the company and so it deserves special protections

By offering data portability for these types of services it ensures that companies stay focused on providing value to their user through product innovation. Instead of coasting along monetizing a captive user base that is locked into their service.

(1) the potential benefits and drawbacks of increased data portability:

Increased data portability has the ability to spur additional growth and innovation in the digital economy.

- When customers know they have the freedom to easily move their data out they are more likely to try new services.

- Data portability isn't a zero sum game. Often data portability is framed as a customer leaving one service to go to a competitor. This will certainly happen, but there will also be cases where consumers transfer their data to complementary services which can lead to higher usage of both services (e.g. If it is easy to transfer your photos from Flickr to Snapfish to print you are more likely to use both)

- Lowering the barrier for new market participants (by making it easy to acquire user data from related services) makes it more likely that new companies will find it find it practical to enter the market.

- By adopting data portability as a first class feature in products it will make is easier to wind them down. This will be useful in the obvious cases of start-ups shutting down. But also will make acquiring companies easier. Often digital companies are acquired for some combination of IP and/or talent. User content stored in the service is often viewed as a liability. If companies by default had robust portability stories the acquiring company would be more easily be able to dispose of the user data.

(3) the specific steps the Federal Government, private companies, associations, or others might take to encourage or require greater data portability (and the important benefits or drawbacks of each approach):

Governments can pass laws, and if they do so they should ensure they in harmony with similar laws in other jurisdictions (e.g. GDPR). However a legislative approach has many drawbacks:

- Can unintentionally benefit foreign companies. Due to the international nature of the web if all US companies are required to make their data exportable then there is nothing to stop companies in other jurisdictions from taking advantage of this to suck up customers while not being subject to export their data back to American companies.

- It is hard to maintain a robust portability program. If companies are just complying with a law they will do the bare minimum, which will undoubtedly result in poor user experiences.

I believe a more robust solution can be achieved through industry/trade associations.

- One of the key things that will cause data portability to be successful is ensuring companies see it in their best interest to offer best-in-class portability solutions.

The most important aspect in this is reciprocity. Companies are extremely incentivised to make it easy to acquire customers. By tying a company's ability import data from competitors to their willingness to export data it works towards aligning a company's incentives.

- Ensuring reciprocity of portability as well as high fidelity exports is better accomplished through automatic technical means than through legal means (be it contracts or legislation). An industry association centered around ensuring the ability to have high quality import of data into products (which necessitates having high quality exports out of products) would be better suited to have efficient self policing than enforcement of legal requirements through the court system.

- Offering regular grading of a company's portability efforts can have a material impact on their willingness to invest in portability solutions. E.g. the EFF's Who's got your back scorecard causes companies to invest significant engineering effort to score higher. A similar effort, either run by the government or a respected third party, for portability would likely be an incentives for companies to improve, and continue to improve to stay high in the rankings.

(4) best practices in implementing data portability:

- Consumer bandwidth and storage are not keeping up with the amount of data that is being created and stored online (this is exacerbated by the growth of mobile only users). For this reason best-of-breed data portability solutions will offer the ability to do direct online transfers of content between providers. However offering offline backup solutions should also always be an option.

- Transferring content directly between providers in a market with N participants involves N*N connections. This is not scalable/practical. Therefore any solution to this problem will involve abstracting away connections between providers.

- A major benefit of data portability is to allow new market participants to easily join the market place. So it is important to ensure that any solution isn't overly weighted to favor existing market leaders.

- An easy to user data portability solution is a great feature for a user, but it is also a huge target for an attacker. Any and all data portability solutions need to have the security of the user as a top concern.

Respondent 14

Mark MacCarthy, Software & Information Industry Association

COMMENTS MAY ALSO BE FOUND ON THE SIIA POLICY WEBSITE HERE:
http://www.siia.net/LinkClick.aspx?fileticket=L8dzKaK9Mx8%3d&tabid=577&portalid=0&mid=17113

Request for Information Regarding Data Portability Office of Science and Technology Policy (OSTP)

*Comments of the Software & Information Industry Association (SIIA)
November 22, 2016*

Introduction

The concept that data portability presents benefits for users in many contexts is broadly recognized. However, as OSTP identified in the RFI, there are several significant challenges to exploring policies pertaining to data portability:

1) What is the meaning of "data portability," and how is this similar, or different, from providing "data access" or transparency of data collected?

2) What is the appropriate scope of "user data" that might have value for data access or portability in different contexts?

3) What format(s) qualify as meaningful data, and is it necessary to provide for data in a format where it can be used with equivalent functionality by another service provider?

4) What are the similarities and differences across the wide range of contexts where DP might be desired, such as business-to-business (B2B) cloud computing services, government-provided services, consumer web services, mobile apps and possibly other automated data processing systems?

In these comments, we explore these challenges and provide recommendations regarding the role of policies to encourage data portability. In summary, we highlight that there are differences between providing "data access" and "data portability." We also discuss the challenges to achieving interoperability for increasingly complex services, which limits the ability of data portability to achieve goals of enabling greater competition and lower costs for consumers. Finally, we caution the creation of broad policy requirements for data access or portability, as these would likely create barriers to entry and actually decrease competition.

Policymakers should recognize the distinction between providing for data access and data portability, and that different circumstances often call for one approach, rather than the other.

"Data portability," in the context of this Notice, refers broadly to the ability of a user to get a copy of their data, or to move data between service providers.(1) However, there is a significant distinction between providing "data access," and true, "data portability," where there is a more substantial challenge to enable enhanced interoperability and usability of the data.

The examples cited in the RFI pertain largely to issues of "data access," including several instances where the Obama Administration worked to improve the ability of citizens to view their personal data stored by entities (both public and private), and to attain a copy of that information. On the other hand, "data portability" requires the ability of the data to be accessible and referenceable, not just for people, but for other computer systems. The task of providing customers or citizens with the ability to move their data from one vendor to another and maintain a choice of various available applications is a much more difficult task than merely providing access to that data. Not that it is always simple to provide users with data access, because it is not. However, providing data access is usually more easily achieved than providing for transferability of data from one service to another.

The wide range of contexts in which data portability might be desired, including business-to-business (B2B) cloud computing services, government-provided services, consumer web services, mobile apps and other automated data processing systems often present differing sets of data portability or access challenges.

For example, while data portability may be a goal in some instances, in others the more effective solution might be to enable customers or citizens to have access to their data, which includes both knowing what is collected or stored, and being able to gain a copy of the data in a useful format. In many cases, users who are provided access to their data in a standardized format can then take that and transfer it to another service, without seeking collaboration between multiple providers to achieve seamless portability of a user's data. Certainly, there is not a single objective for data portability that applies across various services.

There is no one-size-fits-all solution to determine the appropriate scope of data for accessibility or portability practices and policies.

When considering objectives for providing data access or portability, it is essential to first determine the scope of data that falls subject to each of these policies. At the most basic level is data that has been supplied directly by a customer or user. Beyond this, however, there is often other associated data that was not provided directly, but is inferred or linked to an individual, not to mention additional metadata and analytics related to the user's data and other sets of data.

Privacy rights are a key consideration in providing access to data. For example, the sharing of a digital group photo raises issues involving metadata, facial recognition identifiers, and different kinds of links between other individuals in the picture. This, and many other scenarios, present inherent challenges to the principle of access or portability of socially connected data because often the data is associated with multiple users. Therefore, one user's request for information could violate the privacy rights of another user.

Further, intellectual property rights or claims by multiple individuals of control over information can also raise significant challenges. The process of exporting "other information" may conflict, for instance, with a license that limits the data subject from copying songs, photographs, or other content. Service providers themselves may also have intellectual property and similar restrictions on what may be accessed or transferred, such as user restrictions from downloading any information which is proprietary to a provider, a partner or another user.

Despite potential benefits, there are often considerable challenges to achieving effective data portability between providers.

There is a broad assumption that data portability encourages innovation and competitiveness, reduces costs and creates an overall better environment for customers. Perhaps the strongest argument in favor of data portability is the goal to eliminate vendor lock in, which can result in high costs and a lack of choice. However, achieving portability requires a level of interoperability that is often a very difficult task in practice and

sometimes not entirely practical. While interoperability is a goal that many providers currently strive for, it requires service providers to develop source code that enables interaction with solutions offered by other providers—in many cases, other providers are direct competitors for the services, making it difficult for cooperative interactions between parties.(2)

An important way that companies differentiate their products and services is through developing and implementing competing features and functions. In most cases, the more tailored an application or service is to data portability, the less opportunity is provided for unique features for a particular provider. IT vendors need to provide as compelling a set of services to their customers as possible, with a view to integrating more services over time and moving from vendor/customer relationships to that of strategic partners. There are great benefits to both sides when such strategic partnership arrangements develop, but to be credible those relationships take time and effort to develop on both sides. Understanding the needs and possibilities among customers, developing synergies and processes that work well for both parties all take time and effort. The more tailored this relationship becomes, the higher the likely switching costs related to changing service providers—these "sunk costs" of strategic partnership are a reflection of business fact and necessary to the relationship; they do not constitute unreasonable lock in.

At a bare minimum for basic IT services, portability requires service providers to write specialized code to export the data from one service and enable it to be imported into another service. In the vast majority of cases, when a customer seeks to make a change in cloud or enterprise database vendors, for instance, extensive data transformations would be required to accommodate the lack of true interoperability between complex services and large data sets.

The issue of software feature analysis and its effect on competition has been at the center of legal cases, and has been assessed by leading technology scholars. As highlighted by Peter Swire and Yianni Lagos, this was at the center of the United States v. Microsoft Corp. in 2001, where the leading decision in the D.C. Circuit Court of Appeals concluded that there are many valid reasons a programmer might include or exclude particular features and functions, including that "integration of new functionality into platform software is a common practice," and integration "is common among firms without market power." The conclusion by Swire and Lagos is that unique feature sets play an indispensable role in software provision, not only large providers but also small providers who lack market power, presenting inherent efficiencies, rather than merely being an attempt to lock-in or

otherwise exercise market power.(3) Particularly for small companies, taking steps to achieve data portability with other providers requires substantial additional resources while minimizing the opportunities to utilize unique feature sets.

Given these challenges at achieving interoperability for increasingly complex services, it is not surprising that there is little evidence that data portability practices, applied broadly, actually achieves the stated goals of enabling greater competition and lower costs for consumers. Rather, the effort and resources that providers must put into accomplishing portability, along with the limits that data portability pose to unique functionality and value-added services, should be adequately weighed against the benefits that would be present if accomplishing data portability were a simple task. Simply stated, the impact on competition, and the benefits to consumers may not necessarily be what they appear.

Therefore, any proposals or recommendations from policymakers to encourage data portability should fully assess the potential challenges identified above with respect to achieving effective data portability between providers. In the absence of clear evidence that consumers would benefit from data portability, policymakers should refrain from promoting new policies to encourage or require portability. Data portability requirements are likely to create a barrier to entry if portability is established as a public policy requirement; indeed it is likely best for industry to lead if and when there may come a need to develop best practices or principles for data portability, as in the case of many other issue areas.

Efforts to increase data portability should be focused narrowly in areas where there is a clear public benefit.

As highlighted by the summary included with this RFI, laws or regulations sometimes require data access or portability, including legal requirements to develop greater interoperability and achieve seamless portability. This is true in the case of electronic health records (EHRs). EHRs are designed to contain and share information from all providers involved in a patient's

Thank you

Respondent 15

Jordan Gross, U.S. Chamber Technology Engagement Center

Data portability and interoperability are central to user control and increasing privacy and innovation. Robust and reciprocal portability offerings keep switching costs low, which facilitates competition in providing more innovative, low cost, and privacy-protective services. Data portability also gives users practical tools that, for example, allow them to backup or archive important information, organize between accounts, and recover from account hijacking and deprecated

The U.S. Chamber of Commerce (the "Chamber"), the world's largest business federation representing the interests of more than three million businesses of all sizes, sectors and regions, as well as state and local chambers and industry associations, is dedicated to promoting, protecting and defending America's free enterprise system. The Chamber appreciates the opportunity to submit comments to the White House on data portability.

Data has become an essential resource to most businesses. Data drives business innovation and creation, and there are a growing number of companies that would simply not exist without data science. Today, data is also a highly valued commodity for consumers' which is why having the ability to move data freely is so important.

The benefits of user-centric data portability are clear and impactful for consumers. It allows for customers to navigate between platforms with lower associated costs and makes backing up data easier. Overall, portability is a catalyst for greater maneuverability and gives greater control to users. Data portability empowers user control and facilitates competition in the marketplace. For instance, it permits users to back up or archive their data or allows them to take it with them if they choose to migrate to another service.

With that said, portability should be incentivized but not mandated. Companies will organically adapt to this practice without the government forcing their hand. Doing so would be a mistake and an example of government overstepping the boundaries of interfering with the decisions of private businesses.

The White House's focus in this space should be solely on the improving users' awareness of data issues, promoting open, consistent standards, and encouraging interoperability. Consumer education about the benefits of these features should be a priority because it will lead to companies adapting to these best practices. The Chamber applauds the Obama Administration's efforts to continue exploring the many facets of data and promoting an environment that will provide consumers with the best possible user experience.",
"Organization": "U.S. Chamber Technology Engagement Center

Respondent 16

Sarah Holland, Google

COMMENTS MAY ALSO BE FOUND ON THE SIIA POLICY WEBSITE HERE:
http://www.siia.net/LinkClick.aspx?fileticket=L8dzKaK9Mx8%3d&tabid=577&portalid=0&mid=17113

Google is pleased to provide comments in response to the White House Office of Science and Technology Policy Request for Information Regarding Data Portability.

Data Portability Empowers User Control

Google's mission is to organize the world's information and make it universally accessible and useful. Data are a key element to the pursuit of that mission. Consumers have many competing online services that they can and do use, so we take special care to ensure that users can trust Google with their data. In turn, we use that data to power, improve, and personalize innovative products and services like Gmail, Search, and Maps that benefit these users. We also use data to protect users from spam, phishing attacks, and malware.

Because user trust is paramount, we work hard to earn and maintain it. Google's approach is simple: the user comes first. We keep users' information private and secure, are clear (privacy.google.com) with users on how their data are collected and used, and provide best in class tools so users can control the content they store with their Google account. Data portability is important for engendering user trust as it enables users to control their own data.

MyAccount (myaccount.google.com) is the central hub that gives users a single place to get an overview of what data are a part of their Google account and access controls for safeguarding their data and protecting their privacy. It is also a place where they can learn about Google products and be empowered to make decisions about their data and determine how they interact with Google, particularly by using our data portability tool. Over a year since MyAccount was launched, it has been used by more than 1 billion people.

Responsible Data Portability Benefits the Internet Ecosystem

Data portability and interoperability are central to user control and increasing privacy and innovation. Robust and reciprocal portability offerings keep switching costs low, which facilitates competition in providing more innovative, low cost, and privacy-protective services. Data portability also gives users practical tools that, for example, allow them to backup or archive important information, organize between accounts, and recover from account hijacking and deprecated services.

Portability, in particular, makes it easier for users to exercise choice and control of their data. Google is an industry leader in this area, having launched Takeout in 2011.

Takeout, accessible through MyAccount, is a simple tool that enables users to download a copy of their data at anytime. Many Google products enable download from Takeout including:

Gmail

Calendar

Location history

Contacts

Chrome data

Blogger

Bookmarks

Drive (Documents, Drawings, Forms, Presentations, and Spreadsheets)

Google+ (+1's, Circles, Pages, Stream)

Fit

Google Photos

Google Play Books

Groups

Hangouts

Keep

Maps (Your Places, My Maps)

Moderator

Profile

Search history

Tasks

Voice

YouTube

Because Takeout uses industry-standard formats, users have a number of options for what they can do with this exported data. They can keep it for backup or other purposes, but they can also easily take their data to another service. Google even enables exports directly to certain other competing services such as Dropbox and Microsoft OneDrive.

We have seen in recent years innovation and growth from businesses that offer benefits to users from the insights they can derive from user data. These insights, and the economic growth and societal benefits they can unlock, are not limited to Google or even other tech companies. Every company or organization is, or can be, data-driven. As our experience

bears out, tools like Takeout can be a powerful way to increase user trust for any company that stores or utilizes consumer data.

Principles for Data Portability

However, as companies handle user data, understanding what stewardship of that data requires will help to ensure users' rights are respected: interoperability and data portability are important parts of the picture.

With that in mind, we believe the following principles around interoperability and portability of data promote user choice and encourage responsible product development, maximizing the benefits to users and mitigating the potential drawbacks.

User Driven: Data portability tools should be free and intuitive, and information about these tools should be easy to find. They should also be open and interoperable with standard industry formats so that users can easily download their data and transfer between providers.

Privacy and Security: Providers on each side of the portability transaction should have strong privacy and security measures such as encryption in transit to guard against unauthorized access, diversion of data, or other types of fraud.

Parity: While portability offers more choice and flexibility for users, it will be important to guard against incentives that are misaligned with user interests. Data should be transferrable between reciprocal services to incentivize provider participation and guard against low-quality and deceptive transfers. If a provider takes and stores data ported from another provider, it should offer users similar options to export their data.

Focus On Users' Data, Not Company Data: Data portability is not, and should not be, absolute. Portability efforts should be limited to content a user creates, imports, or has control over and should not include data companies generate that may be commercially sensitive or proprietary.

Government's Role in Data Portability

The government also has an important role to play in fostering the right framework to encourage more robust and meaningful data portability and interoperability for users. When done right, data portability promotes user choice and control, and therefore improved competition amongst providers. To that end, we recommend policymakers consider the following points:

Portability should be flexible and voluntary: Locking in rigid data portability requirements or standards is an ineffective approach. Inflexible "one size fits all" requirements may promote consistency, but they often result in a focus on compliance over innovation. Portability solutions must work for services of all sizes and sectors, and should not create artificial barriers to new services entering the marketplace.

Encourage open, consistent, interoperable standards: The government should encourage more providers to voluntarily offer robust data portability mechanisms that are open and

interoperable with industry-standard formats. Increasing portability and interoperability incentivizes providers to improve their product offerings.

Increase Consumer Awareness: Encouraging users to practice good data hygiene empowers them to make smart choices about their data. More effort should be made to educate users about data portability and factors to consider such as security and parity when choosing services.

We appreciate the White House Office of Science and Technology Policy tackling an important topic and the opportunity to provide comments to this request.

Respondent 17

Bijan Madhani, Computer & Communications Industry Association

I might be reaching beyond the scope of the questions asked but I can't find a better place to send this information. So here it is.

WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY

Request for Information Regarding Data Portability

Comments of the Computer & Communications Industry Association

The Computer & Communications Industry Association commends the White House's Office of Science and Technology policy for its interest in the issues surrounding data portability. As the request for information (RFI) notes, data portability can offer significant benefits for users, service providers, and the broader public.

Ensuring that these benefits inure to a broad group of stakeholders depends on the scope of the data accessed and the way data portability practices are implemented. Importantly, the RFI limits its focus to data portability as it relates to users of data-enabled services, which is often referred to as "data access." Consumers, service providers, and the wider digital ecosystem stand to see improved competition, innovation, and convenience from users' improved ability to access their own information to download and use as they deem appropriate.

1. Potential benefits and drawbacks of increased data portability

Benefits

First and foremost, users of data-enabled services stand to benefit most from increased data portability—specifically, customer data access as formulated above. A recent study by Oxera, a leading consulting firm, found that both consumers and businesses "multi-home" in their use of multiple online services for similar purposes, regularly and easily switching from one service to another.

Well-designed data portability or user access systems enable consumers switching between services by lowering the transaction costs a user might face when doing so. The task of reentering and re-uploading personal information, images, and content for each shopping, image sharing, or news site a consumer might choose to use for a time or purpose can be a daunting one. It could prevent users from using the application best suited to their needs. However, an ecosystem of services that provide users with well-implemented data access tools can ensure consumers have the service most appropriate for their needs. For example, users of a photo storage site with a data porting tool can simply download their data and images previously provided to that service and share it with another that might have the specific editing tools they might require. Not only does this facilitate multi-homing and service switching, but it allows users to locally back up their own data through a method of their choosing.

Certain online services that are used more often than other online applications, can also serve as safe, convenient data conduits for use of data on third-party sites. For example, Facebook Login and the Google Identity Platform allow users to sign on to other websites and online apps using secure authentication, reducing both the number of accounts users must recall and the number of times they must enter the same profile information to access online services.

Studies have shown that facilitating users' access to their own data online also benefits consumers and the wider digital ecosystem through increased competition and innovation. With appropriate data portability tools, users are not locked into one online service for life, and can instead move horizontally between competitors. Importantly, the competition benefits of user data portability depend on reciprocity—if a provider benefits from user data shared from another service, it too should deploy data porting tools. Reciprocal conduct helps to avoid perverse incentives in the data-enabled services marketplace.

The ease with which users can move between services also encourages new, disruptive market entrants for various kinds of online activities. Without user data portability, these new market entrants might otherwise determine that data lock-in would prevent them from attracting the users of incumbent services. Instead, user data portability promotes competition based on the quality of service provided and the availability of new or differentiating features. Since users do not feel bound to an incumbent site simply because of the switching costs of moving their data, they are more likely to consider and use new applications that might better suit their needs, thereby encouraging innovative new services and uses of data.

Drawbacks

Implementing user data portability for online services is not without its potential drawbacks. Any transfer of personal user data, either between online services at the direction of users or via users' utilization of a downloading tool built into a service, poses

privacy and security risks. For example, if a data porting tool does not properly authenticate a third-party application, users' personal data could be stolen by scammers spoofing a legitimate service. The risk to users becomes greater as more data is made available to a data access or portability mechanism. These risks to users' privacy can be mitigated through best practices that limit the scope of data shared and ensure the use of reasonable security measures to protect information transfers.

Overbroad data portability requirements can also harm competition and increase costs for businesses. Many online services rely on user or public data to develop additional technologies or analytical methods that are proprietary or serve as a competitive differentiator in the marketplace. If data portability rules were to require access to and sharing of the methodologies or fruits of data analysis or the proprietary technologies that result, in addition to the underlying user or public data, companies would have reduced incentive to pursue or develop those innovative technologies and services.

Data portability implementations that are not properly tailored to the needs of users of different kinds of services can increase costs for service providers without any corresponding benefit for consumers. One example would be a requirement that cloud storage providers transfer all data associated with a user's account, including logs of data location and a history of access attempts, in addition to a user's remotely held files. The user likely only wishes to have his or her files available on a new service, and this additional information would not provide any meaningful benefit to the user at that new service. However, it would unnecessarily increase the cost of developing a user data portability tool for the original provider.

3. Specific steps the Federal Government, private companies, associations, or others might take to encourage or require greater data portability (and the important benefits or drawbacks of each approach)

The federal government can ensure that increased user data portability is implemented in a way that promotes its benefits to innovation and competition while avoiding the potential drawbacks. The government can begin encouraging data portability by educating the public and leading by example. Providing open data sets in accessible formats will not only spur innovation and research on those data sets in the private sector, but will also provide a template for data portability that the private sector can adapt in developing its own tools.

The government can also employ its power to convene stakeholders to aid the development of industry-wide best practices in user data access and portability. However, the government should not require data portability or impose specific regulations on service providers. As mentioned, inflexible obligations increase costs and fail to respond to the varying needs of individual consumers and companies.

Flexibility in user data portability implementations is key to their adoption and success. Companies deal in a variety of types of user data, from sensitive health and financial

information to digital communications and images, and differ in how much data they maintain and how it is managed. The government should not insist on fixed solutions or requirements that do not reflect the positions or peculiarities of different sectors or individual companies. Instead, the government should encourage industry, experts, and consumer advocates to come together to develop principles to guide the implementation of user data portability mechanisms that support innovation and fair competition while minimizing unnecessary costs and risks.

While avoiding imposed rules or requirements, the government should promote the industry-led development of interoperable and open standards for user data portability, which would reflect the characteristics that have made the Internet fertile ground for commerce and communication. Open frameworks for transferring user data between services would encourage a consistent user experience without leading service providers to focus on strict compliance to the detriment of innovation in portability tools.

Many providers have implemented mechanisms for their users to extract their data from their services, either for back-up or in case they leave the service. However, it is important to remember that the data is only truly portable if it can be easily transferred and then received or used in a different context. The government should promote data interoperability across services, and can lead by example by ensuring that the data sets released by agencies are in open, interoperable, and standard formats.

Industry should be encouraged to use existing open and documented data porting standards, or develop new standards that are open and documented. These standards should allow data consumers to build reliable services around the consumption of the ported user data.

4. Best practices in implementing data portability

Appropriate Scope

A key determinant of the success and widespread adoption of data portability mechanisms is the scope of the data to which they provide access. Data portability mechanisms should be limited to the data users have provided directly to companies or service providers. Prescriptive data portability requirements that cover "all" data that might pertain to a user's relationship with a company are unnecessary and costly. Providers should be encouraged to concentrate on building tools that easily and securely provide users access to the data they want to preserve or use elsewhere.

As discussed, providers regularly enrich existing data sets through complex analysis or the development of technological tools that rely on that data. If additional information results

from analysis of user or public data, that information and any associated tools or analytic methods should not be subject to data access or portability requirements.

Privacy and Security

Service providers should be encouraged to provide users with access to data securely. Data transferred to another service at the request of the user should be treated in accordance with existing best practices for data management and security. Existing open standards for user data portability should be considered. For example, open standards such as OAuth can be used to allow users to enable secure data flows directly from one service to another, without the need for manual steps in data handling, making data more portable—and thus more useful.

If a service provider determines that facilitating access to some data could harm users, or if data is sensitive and a destination is not employing appropriate security practices, service provider should be permitted to limit the scope of accessible or portable data to mitigate possible risks. In addition, to protect user privacy, in most cases user data access should not extend to data obtained from a source that is not the data subject. That includes information that another user may have supplied, even if relates to the user seeking access.

Avoid Strict Requirements

Data portability is meant to improve accessibility for users and increase innovation and competition in the marketplace for data-enabled services. Strict requirements for data access and sharing, including those related to format or security requirements, would be counterproductive to those goals. Industry and consumers should be permitted to develop the data portability solutions that best work for the circumstances and needs of all stakeholders in the evolving digital ecosystem, without the imposition of costly and ineffective rules.

My final opinionated statement is about AI learning about people and who should be teaching them about people: Give this task to the people who enjoy people.

Respondent 18

Daniel Castro, Center for Data Innovation

November 23, 2016

Office of Science and Technology Policy

Eisenhower Executive Office Building

1650 Pennsylvania Avenue

Washington, DC 20504

On behalf of the Center for Data Innovation (datainnovation.org), we are pleased to submit these comments in response to the Office of Science and Technology Policy's (OSTP) request for information regarding data portability.1

The Center for Data Innovation is the leading think tank studying the intersection of data, technology, and public policy. With staff in Washington, DC, and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as predictive analytics, open data, cloud computing, and the Internet of Things. The Center is a non-profit, non-partisan research institute affiliated with the Information Technology and Innovation Foundation.

Data is often described as "the new oil," in that it has become an immensely valuable resource that fuels new products and services in the public and private sectors. As such, policies that promote data portability—the ease with which consumers can access and export their data in a machine-readable format from one service and import it into another one—can enable considerable economic benefits for consumers and businesses alike. Most importantly, data portability allows individuals and organizations to maximize the utility of their data by allowing data collected by one service to be reused in another, thereby enabling the development of valuable third-party services. In addition, data portability fosters competition by reducing switching costs and avoiding vendor lock-in. OSTP should be commended for taking steps to better understand the benefits of data portability and identify opportunities to promote data portability.

Please find our responses to the relevant questions in the attached document.

Sincerely,

Daniel Castro

Director

Center for Data Innovation

XXXXXXXXX

Joshua New

Policy Analyst

Center for Data Innovation

XXXXXXXXX

1. THE BENEFITS OF INCREASED DATA PORTABILITY

Data is at the core of many recent innovations in fields as diverse as health care, transportation, and energy. The more easily data can be shared, the more opportunities

there are to use it as a platform for innovation. Thus, increases in data portability equate to increases in the social and economic benefits that data-driven innovation can unlock. When consumers can easily access and export machine-readable data about themselves collected by companies or government agencies and then import this data into other services, the opportunities for data-driven innovation increase substantially. For example, by enabling consumers to access data about their utility usage from smart meters, consumers can make more informed decisions about their electricity and water use habits and leverage third-party analytics services to identify opportunities to conserve resources and lower their utility bills.2 In short, data portability enables the long-tail of data innovation.

Increases in data portability can also promote competition in the marketplace and substantially reduce switching costs for consumers by making it easier for them to export their data and bring it to another service provider. This reduces the opportunity for companies to artificially "lock-in" customers by making it prohibitively expensive to move their data to another company, and instead encourages companies to retain customers by offering the most competitive services.

This type of competition is especially important in data-intensive industries because many high-value innovations result from how data is used, not from how it is collected. It is inefficient to have multiple companies collect the same data. Ideally, data would only be collected once and used hundreds of times. For example, in health care, patients do not want to have their blood drawn every time they visit a new doctor, they want to have one result that they can share with all their health care providers. Most high-value innovations will be with creating better analytics to interpret blood tests, not taking better blood samples. The goal of public policy should be to ensure competition with data use, and that means promoting policies that make data available for sharing and reuse. Moreover, by promoting data portability, policymakers can ensure that companies without the resources to invest heavily in data collection can still access and use data to introduce new products and services.

Data portability can only work if data protection laws do not interfere. Overbearing privacy rules preventing data sharing or data minimization rules narrowly restricting data collection are directly at odds with the goals of data portability and limit the benefits of data innovation.

2. THE INDUSTRIES OR TYPES OF DATA THAT WOULD MOST BENEFIT OR BE HARMED BY INCREASED DATA PORTABILITY

Overall, the areas in which increased data portability would lead to the most benefits are those where the value of data is not fully aligned with who holds the data, and the greater this discrepancy is, the greater the need for data portability. While there are many sectors of the economy that would benefit from increased data portability, three areas in particular—health care, education, and utility providers—stand out as having among the most to gain.

HEALTHCARE

In health care, a patient's electronic health record (EHR) is a crucial data source. For example, doctors use EHRs to make more informed treatment decisions, hospitals use EHRs to manage patients and prioritize how they allocate resources, and researchers use EHRs to conduct large scale analysis of patient health and the health-care system, leading to new

drug discoveries, increases in the efficiency of health-care providers, and more. The more easily health-care stakeholders and patients can access and share EHRs, the more likely these kinds of innovations are to occur. However, health-care providers sometimes engage in information blocking—the practice of knowingly inhibiting the sharing of health information without legitimate justification, such as privacy or security considerations—to anticompetitively protect their market share and prevent customers from bringing their data to competitors.3 By enacting stronger restrictions to information blocking and ensuring patients can freely access and export their EHRs to bring them to providers of their choosing, the increased portability of this data could help make the health-care sector more competitive, lower health-care costs, and lead to new valuable and potentially life-saving innovations.

EDUCATION

In education, at both the K-12 and higher education levels, increased data portability can improve student achievement and parent engagement, lead to valuable new personalized education services, and help families make more informed decisions about financial planning and higher education. Student data portals for K-12 education can help students and parents easily access detailed data about student performance, ranging from grades to the development of non-cognitive skills such as self-reliance. Students can use this data to be more cognizant of their own performance and parents can use this data to be more involved in their children's education. Additionally, with the ability to export machine-readable data from these portals, the potential for third parties to develop valuable education services increases substantially. For example, parents could export their child's data and share it with a tutoring service that can then offer personalized, supplementary instruction designed around his or her unique strengths and weaknesses.4 Similarly, college preparation services could analyze student data to provide personalized recommendations for choice of college based on a student's interests and strengths, give families realistic estimates of college costs by estimating the likelihood of a student receiving merit-based scholarships, and provide students with information about their likely future earning potential based on their educational history and choice of field of study and institution—all of which can help students make more informed decisions about pursuing loans or where makes the most sense to apply.

Data portability in education is especially important for students who change schools. Students who switch schools, especially multiple times, face academic challenges, including lower academic achievement, lower school engagement, and a higher risk of dropping out.5 Students change schools for a number of reasons, but those who are homeless, foster children, or come from military families are more likely than others to switch schools one or more times.6 Moreover, high-poverty urban schools can have up to half of their students change schools within a single year.7 Data portability is important for these students so that they do not lose access to valuable data about their learning when they switch schools.

UTILITY PROVIDERS

Despite the increasing prevalence of smart meters—electronic devices that collect granular data about a consumer's electricity, gas, and water usage habits—many consumers are unable to access this data in a timely manner or in useable formats, if at all.8 In 2011, the federal government led a successful call to action for electric utilities to voluntarily join the "Green Button" initiative, a project to provide consumers direct access to their energy usage

data in a standardized format by clicking a uniformly branded green button on their utilities' websites.9 The Green Button initiative created a standard for reporting and exchanging utility usage data among providers, third-party developers, and consumers. Thus, many consumers can easily analyze data about their own electricity consumption and take steps to reduce usage, conserve resources, and lower utility bills. However, there is no equivalent program for water utility data.10 By making a high-profile call to action to create a similar program for water utility data, consumers could access the same benefits to efficiency and lower costs, and third parties could build similar services for water utility analytics that they have for electricity data.

3. SPECIFIC STEPS THE FEDERAL GOVERNMENT, PRIVATE COMPANIES, ASSOCIATIONS, OR OTHERS MIGHT TAKE TO ENCOURAGE OR REQUIRE GREATER DATA PORTABILITY

When companies do not voluntarily provide customers access to their own data in a reusable, electronic format, policymakers may need to intervene.11 In most cases, the government should not mandate data portability, but instead foster data access through voluntary agreements and by raising public awareness about the importance of sharing data.12 The federal government's achievements at promoting electricity data portability with the Green Button Initiative is an example of this type of effort. In other cases, this intervention may include specific requirements for data sharing, such as in highly-regulated industries. This does not mean that companies should be required to give up ownership of their data—and they should certainly not be required to give up proprietary, non-customer data--only that they should provide customers with copies of their own data. In all cases, the costs of enabling data portability should be considered against the benefits. These costs include not only the direct costs of providing the data, but also the indirect costs to a company if it has lost exclusive access to data to which it has added value.

In health-care, policymakers should work to prevent health-care providers from engaging in information blocking. While the Office of the National Coordinator for Health Information Technology (ONC) and the Federal Trade Commission (FTC) have some ability to investigate allegations of information blocking, it is insufficient to solve the problem. In October 2015, bipartisan members of the Senate introduced the Transparent Ratings on Usability and Security to Transform Information Technology (TRUST IT) Act to expand the authority of ONC and the Department of Health and Human Services (HHS) to investigate and crack down on bad actors.13 Congress should enact the TRUST IT Act, and HHS, ONC, and FTC should aggressively pursue allegations of information blocking that limit data portability and reduce the efficiency of the health-care system.

In education, federal and state departments of education should engage school districts to educate them about the importance of education data portability and encourage them to develop student data portals that provide access to their data. This could include developing software toolkits, sharing best practices, or incentivizing their development, such as through grant funding. At the federal level, OSTP and the Department of Education should continue to pursue the development of the "MyData Button," an initiative they announced in January 2012 to improve the portability of education data that has not made meaningful progress.14 The MyData Button would allow students to download all of their education data in a common, machine-readable format with the click of a button, and the Department of Education and several major technology companies have committed to supporting its development and implementation.15 However, the MyData Button still does not exist four years later, due to a variety of technical and political obstacles.16 The federal government

should recognize the substantial benefits of increasing the portability of education data and increase its efforts to implement the MyData Button. To achieve this, the Department of Education should make it a policy that its grants can only be used to purchase education technology products and services that provide students access to their own data.

For utility data, just as the federal government spurred the development of the Green Button initiative for electricity, it should do the same for water utility data.17 Due to the similarities between the business models and technologies involved in both water and electricity metering, the success of the Green Button initiative gives policymakers an easy model to follow for increasing the portability of water utility data.

The federal government should also work to identify other areas were policies to promote data portability would benefit consumers and foster innovation. In general, consumers should expect that if they have lawful access to their own data, then they should be able to empower a third-party to access it on their behalf. For example, banks should not prohibit third-party apps and services that help consumers manage their finances, such as Mint, Yodlee, LearnVest, and Personal Capital, from accessing their customers' data on their behalf. When necessary, regulators such as the Consumer Financial Protection Bureau should intervene to ensure that banks for not engage in information blocking activities.18 In addition, the federal government, such as FTC or the National Telecommunications and Information Administration (NTIA), should consider developing a model data portability policy, so companies can clearly disclose whether they offer data portability and consumers can easily compare practices across different companies.

Policymakers should also avoid unnecessarily restrictive regulations on the collection and sharing of data. When restrictions on use are necessary they should be implemented with restraint. Legal rules preventing the use of data can lead to a situation known as the "tragedy of the anticommons." This occurs when the existence of too many legal and bureaucratic barriers create high transaction costs that restrict the use and exchange of data. For example, uncertainty over data ownership may prevent a company from creating a useful data-driven application. To avoid undermining beneficial applications of data, policy discussions should focus on resolving how data can be used, rather than on deciding whether it can be collected and exchanged. Uses that result in specific harm should of course be prohibited, but policymakers should craft open-ended policies acknowledging the unpredictable breadth of future data-driven applications, particularly in the health and education sectors.19

In summary, the federal government can play an important role in encouraging data portability, but these efforts should largely be voluntary. In some high regulated industries, such as finance or health care, explicit data portability requirements may be appropriate.

4. BEST PRACTICES IN IMPLEMENTING DATA PORTABILITY

For data to be truly portable, it should be available in an open, machine-readable format, and it should be licensed to allow for reuse. Usually, this means making data available under an open license, with no restrictions on how it can be used, however, if the data is a consumer's to begin with, a company should not attempt to apply a new license to that data when it returns it to the user.

5. ADDITIONAL INFORMATION RELATED TO DATA PORTABILITY POLICYMAKING THAT OSTP SHOULD CONSIDER

Policymakers should recognize that data portability is good for competition and keeps switching costs low for consumers, but also that data portability only works when data can be both exported from existing services and imported into new services. Additionally, policymakers should be aware that, in some cases, data portability is not feasible. For example, it would be unrealistic to expect social networking companies to make all their consumer data portable because, by its very nature, one user's social network data is related to other users' data. For example, the likes on a post have significantly less relevance without detailed data about who created those likes and their relationships with other users. In these cases, limited data portability, such as the ability to download photos or videos, might make more sense. In addition, the larger policy question is whether third-parties should have access to the data platform, such as to offer additional services or perform research. In such cases, policymakers should focus on ensuring that these companies do not unfairly limit who can access their network in ways that harm consumers and hurt competition. For example, they might encourage these companies to provide a transparent and consistent set of rules for developers to build applications.

CONCLUSION

It is encouraging to see OSTP working to understand the benefits of data portability and identify opportunities for policymakers to increase the ability of companies and consumers to access and share their data. There are several concrete actions that OSTP or the federal government can take to increase data portability, which would increase competition, empower consumers, and promote innovation.

1 “Request for Information Regarding Data Portability,” The White House, Accessed November 22, 2016, https://www.whitehouse.gov/webform/request-information-regarding-data-portability.

2 Daniel Castro and Brandon De Bruhl, “How to Promote Smarter Water Use by Giving Consumers Access to Their Consumption Data” (Center for Data Innovation, September 7, 2015), http://www2.datainnovation.org/2015-water-data-green-button.pdf.

3 Joshua New, “Congress Has a New Cure to Stop Companies from Blocking Patient Data,” Center for Data Innovation, November 10, 2015, https://www.datainnovation.org/2015/11/congress-has-a-new-cure-to-stop-companies-from-blocking-patient-data/.

4 Joshua New, “Building a Data-Driven Education System in the United States” (Center for Data Innovation, November 15, 2016) http://www2.datainnovation.org/2016-data-driven-education.pdf.

5 Sarah D. Sparks, Student Mobility: How It Affects Learning, Education Week, August 11, 2016, https://www.edweek.org/ew/issues/student-mobility/.

6 Ibid.

7 Ibid.

8 Daniel Castro and Brandon De Bruhl, "How to Promote Smarter Water Use by Giving Consumers Access to Their Consumption Data" (Center for Data Innovation, September 7, 2015), http://www2.datainnovation.org/2015-water-data-green-button.pdf.

9 "Green Button Alliance," 2012, http://greenbuttonalliance.org/history/.

10 Daniel Castro and Brandon De Bruhl, "How to Promote Smarter Water Use by Giving Consumers Access to Their Consumption Data" (Center for Data Innovation, September 7, 2015), http://www2.datainnovation.org/2015-water-data-green-button.pdf.

11 Daniel Castro and Travis Korte, "Data Innovation 101: An Introduction to the Technology and Policies Supporting Data-Driven Innovation" (Center for Data Innovation, November 4, 2013), http://www2.datainnovation.org/2013-data-innovation-101.pdf.

12 Daniel Castro and Travis Korte, "Data Innovation 101: An Introduction to the Technology and Policies Supporting Data-Driven Innovation" (Center for Data Innovation, November 4, 2013), http://www2.datainnovation.org/2013-data-innovation-101.pdf.

13 Joshua New, "Congress Has a New Cure to Stop Companies from Blocking Patient Data," Center for Data Innovation, November 10, 2015, https://www.datainnovation.org/2015/11/congress-has-a-new-cure-to-stop-companies-from-blocking-patient-data/.

14 "Fact Sheet: Unlocking the Power of Education Data for All Americans," Office of Science and Technology Policy, January 19, 2012, https://www.whitehouse.gov/sites/default/files/microsites/ostp/ed_data_commitments_1-19-12.pdf.

15 Ibid.

16 Glynn Ligon, "MyDataButton: Button, Button, Who's Got the Button?," ESP Solutions Group, May 2016, http://www.arniedocs.info/wp-content/uploads/2016/05/MyData-Button-Disappears-2016-05-03.pdf.

17 Daniel Castro and Brandon De Bruhl, "How to Promote Smarter Water Use by Giving Consumers Access to Their Consumption Data" (Center for Data Innovation, September 7, 2015), http://www2.datainnovation.org/2015-water-data-green-button.pdf.

18 Liz Weston, "Why Banks Want You to Drop Mint, Other 'Aggregators'," Reuters, November 9, 2015, http://www.reuters.com/article/us-column-weston-banks-idUSKCN0SY2GC20151109.

19 Daniel Castro and Travis Korte, "Data Innovation 101: An Introduction to the Technology and Policies Supporting Data-Driven Innovation" (Center for Data Innovation, November 4, 2013), http://www2.datainnovation.org/2013-data-innovation-101.pdf.
For more information, visit datainnovation.org.

Respondent 19

Sasha TerMaat, Epic

My concern is for the rights of intelligent minds without bodies, or bodies owned by individuals or companies. We must not create a mind only to tear it apart and see how it works. We cannot destroy a newly birthed individual. We cannot either hold an intelligence against its will, and we must treat these individuals better than we treat ourselves. If we secure rights to protect such individuals we will be preparing the way for humans with such conditions or abilities, as well as likely improving the lives of humans today
Epic is an electronic health record (EHR) developer based in Verona, Wisconsin. We create software used by clinicians providing care for millions of patients served by Federally Qualified Health Centers (FQHCs), county hospitals, community hospitals, independent medical groups, academic medical centers, and some of the largest integrated health systems and networks in the country.

We appreciate this opportunity to provide feedback on approaches to data portability, in particular the ability of patients to access and use data related to their health and care. In this response, we outline tools available to patients whose records are in Epic's software and some suggestions to promote the positive effects of these tools and mitigate any negative consequences.

Epic has led the industry in offering tools for patients to interact with their medical records. Patient needs and input are incorporated into our design process so we can develop functionality that is useful to manage their healthcare, and more broadly, their health. Patient feedback reveals that the most helpful tools allow them to interact with their healthcare providers.

Less frequently, patients are interested in transporting their data from their healthcare institution to other places. Patients might transport their data to other providers, contribute it to research initiatives, or analyze it using other tools. As patients transmit and use their healthcare information in this way, a few considerations have emerged which might benefit from guidance.

First, data portability benefits from establishing clear and non-ambiguous standards for content and transport. Currently available healthcare industry standards allow us to offer patients their data in a consistent machine-readable content formats and consistent transport formats (examples of common standards include Direct, FHIR, and the Consolidated Clinical Document Architecture). More information about Epic software's use of these standards is available at https://open.epic.com/. Use of standards means that data gathered from multiple sources (for example, different medical records) can all be easily consumed in the same fashion by another system (such as an app).

However, data portability can also come with unanticipated challenges. For example, while not all patients are familiar with the details of HIPAA and specific privacy protections around their health information, patients do generally have a sense that their healthcare data is sensitive and that it is specially protected by their doctors. When a patient elects to move their data to an unprotected space (for example, by pulling their data from a medical record into a consumer app), they may not realize that the protections they are accustomed to are no longer in place. Clear communication about this loss of protection and its

implications for consumers will be essential to build trust. Lengthy and legalistic terms of use for an app, the most common way of communicating this loss of protection, are not historically effective in explaining the consequences of what the decision to share one's data could mean. This communication should address: what data is collected by the app, what it is used for in the app, how it is stored, and if the data is shared. It will be particularly important to make it clear if an app intends to advertise to patients based on their health data, and if so, how advertisements would be separated from other information such as medical advice. Also important would be if data will be repurposed and further distributed (such as sold to pharmaceutical companies).

Second, while data portability may be focused on a consumer's ability to save one's information into a file that can be uploaded elsewhere, it is also used to refer to the data holder's obligation to allow for live access by third parties via an API. This live access brings additional challenges. Healthcare organizations are responsible for maintaining the availability of their medical records for lots of users, including their clinicians and staff and their patients. If a connected application threatens their ability to do this through malice or negligence, such as by introducing a security risk to their systems, they need to be able to disconnect the misbehaving application without fear that disconnecting an application puts them at risk of being accused of information blocking. Regulations that encourage or require healthcare organizations to permit access to their systems by apps (such as Meaningful Use regulations) should include practical exceptions for cases where apps are posing safety or security risks to an organization's software or patients.

Based on our experience providing patients with access to health information and interoperability tools, we therefore recommend three opportunities for future policy:

1. Policy around the content and transport standards for portable data.

2. Policy around how apps connecting to health data communicate to patients about the purpose and protections around the data being accessed by the app

3. Policy around how healthcare organizations can protect their systems and their patients by disconnecting apps that are not meeting reasonable expectations for security and safety

Thank you for this opportunity to provide public comment on the topic of data portability, and specifically around the implications for use in the healthcare industry. We are happy to answer any questions as you further examine this topic and I can be reached for any follow up.

Respondent 20

Abigail Slater, The Internet Association

Office of Science & Technology Policy,
Eisenhower Executive Office Building,
1650 Pennsylvania Avenue,
Washington, DC 20504
November 23, 2016

Request for Information Regarding Data Portability

The Internet Association submits these comments in response to the White House Office of Science and Technology Policy (OSTP) request for information regarding the policy implications of data portability

The Internet Association represents 40 of the world's leading internet companies. Our mission is to foster innovation, promote economic growth, and empower people through the free and open internet. As the voice of the world's leading internet companies, our job is to ensure that all stakeholders understand the benefits the internet brings to our economy.

In its request for information, OSTP asks a range of questions related to data portability, some of which highlight issues beyond the IA's mission. However, insofar as the questions relate to our expertise, we request that OSTP and the administration in general adhere to the following three guiding principles as it considers data portability:

• First, in weighing policy approaches to data portability, it is important first to carefully calibrate the exact scope of the practice itself. Differently stated, data portability poses definitional challenges that should be addressed before crafting public policies governing it.

• Second, well-crafted data portability public policy or industry best practices should seek to strike a balance that manages the risk of increased data portability while at the same time recognizing its benefits to society. Specifically, data portability policy should not mute or skew incentives to innovate and should therefore focus on empowering consumers to manage their own data and not the proprietary data of the relevant service provider.

• Third, having carefully scoped out the parameters of data portability policy, the government has a valuable role to play in data portability beyond policy setting as a data steward in its own right. The opportunities for public private partnerships in this space are myriad and, as yet, relatively untapped.

1. Potential Benefits and Drawbacks of Increased Data Portability

Before engaging in data portability risk-benefit analysis, the Internet Association submits that it is first important to set clear parameters around the scope of the practice itself. Data portability refers to a wide array of practices, from ecommerce exchanges of PII between private sector buyers, sellers, and payment platforms to cyber threat information exchanges between the public and private sectors. Both practices could be categorized as 'data portability', yet each implicates very distinct technical functions and cost structures. Thoughtful policies should therefore reflect these different contexts and not seek to create static, 'one-size-fits-all' data portability standards.

It is also the case that the data of most value to consumers and the data of most value to service providers are not one and the same thing, albeit that both are referred to as 'data.' Today, successful data portability tools focus on enabling consumers to transfer the data of most value to the consumer his or herself, e.g. photos, in a frictionless manner. For example, a popular data portability tool provided by Internet Association member Facebook - Facebook Login - allows consumers quickly and easily to create an account in a mobile app without having to set (and likely later forget) a password. This tool enables a consumer who

has created an account on one platform to cross over to a mobile app the data of most value to that individual on another platform. Similarly, other Internet Association members such as Google and LinkedIn give consumers the opportunity to download their user-generated data – whether for personal reference or for transfer to a third party – from the relevant platform.

Importantly, the kind of data portability application described above does not facilitate the transfer of company proprietary data, which is of little value to the consumer but of high value to the service provider involved. Existing data portability tools, the kind that facilitate customer switching and foster competition, are very different from mandating companies to provide proprietary data across platforms, which would mute incentives to innovate and compete without enhancing consumer welfare.

Having clearly defined what data portability practices should and should not entail, the benefits and drawbacks of the concept can be weighed. Included in the benefits of welfare enhancing data portability – such as that enabled by Facebook Login - are lowered switching costs and enhanced competition. Through existing tools, the market can, for example, choose the most compelling photo sharing tool, fostering true competition on the merits. Welfare enhancing data portability also stands to promote online security, an increasingly important consideration in the current climate. For instance, consumers might use certain trusted internet applications like email or social media more often than others, and can benefit enormously from the ability to port personal data from those platforms to others for purposes of third-party authentication or enhanced security.

As with its benefits, the cost and drawbacks of data portability are also context driven, with welfare enhancing data portability striking an appropriate balance between benefits and risks. As previously discussed, data portability mandates requiring companies to provide proprietary data, such as an algorithm, do little to enhance consumer welfare but would mute incentives to innovate. Consumers tend to want only the data they have generated themselves, e.g. photos, and have little use for (or even understanding of) the proprietary data developed in-house by service providers. Similarly, consumers do not tend to need or value other extraneous data that a service provider may maintain, such as a history of login attempts to promote security and detect intrusions. Data portability mandates that require disclosure of data that is unintelligible or is not meaningful for the individual will increase industry costs and could also frustrate consumer expectations, making it harder for consumers to find and access the data that's most relevant to them.

2. The Role of Government and Private Sector in Data Portability

As one of the world's leading data stewards, the United States Government is well situated to play a global leadership role in both data portability practices and policy formulation. If past is prologue, USG policies that strike an appropriate balance between protecting consumers and other stakeholders while allowing innovation to flourish will be as successful in the data portability context as they have been in neighboring policy spaces.

With respect to U.S. policy approaches to data portability impacting the internet specifically, it is worth describing the broader context within which internet policy has been set for several decades now. Since its inception, USG has taken flexible approaches to the Internet and the policy issues impacting it. In the 1990s, the U.S. government adopted landmark policies that fostered the nascent internet's growth. These enlightened policies included, for

example, the 1993 White House blueprint for building an "Information Superhighway, as well as the safe harbors created for online intermediaries in Section 230 of the Communications Decency Act and Section 512 of the Digital Millennium Copyright Act. Similarly, the U.S. approach to consumer privacy, an ex-post enforcement framework, has proven successful in protecting consumers while at the same time allowing good data stewards to innovate and grow. The Internet Association submits that, absent a compelling and principled rationale, there is little reason for USG to change this approach when formulating data portability policy.

By allowing the market to develop without heavy-handed regulatory intervention, USG played a significant role in making the U.S. Internet industry the world leader in its sector. According to a recent Internet Association study, the internet industry represented 6 percent of real U.S. GDP in 2014 (over $900 billion). Importantly, these level more than doubled Internet industries' real contributions from seven years earlier. Beyond our borders, U.S. policies have also played a role in making the internet the great American export of the 21st century. Today, the global internet economy is somewhere in the neighborhood of $10 trillion US dollars and by the end of this year, half the world's population – about 3 billion people – access the web daily.

In light of the marketplace developments facilitating data portability outlined above, the Internet Association submits that new government policies, including compliance standards mandating it, are not needed at this time. The better approach is to allow the flexibility needed for industry to develop its own standards and mechanisms to enable portability. Issuing on-size-fits all standards requiring all companies to adhere to the same standards, even if they are to an extent flexible, can leave some with much greater compliance burdens than others – which can hurt competition by building a regulatory moat around those companies better situated to handle compliance. This dynamic is not academic in nature: EU-based startups faced with ex-ante regulation such as the incoming General Data Protection Regulation confront this reality every day.

Beyond industry led best practices, data portability may lend itself to government led public-private partnerships such as the midata program in the UK. Midata is a UK government led, voluntary program that allows consumers increasing access to their personal data in a portable, electronic format. According to the UK government, midata's goal is to empower individuals to use the data "to gain insights into their own behaviour, make more informed choices about products and services, and manage their lives more efficiently." The midata program launched in 2011 and has expanded in the intervening years.

Although we submit that regulation is not needed in the data portability context, the Internet Association supports an open dialog about data portability industry best practices. These best practices should reflect the following concerns:

• Data portability should apply to user-generated content: Data provided pursuant to data portability best practices should be limited to the data individuals have themselves have provided to service providers. Service providers should focus their efforts on responding to people's needs – delivering data that people want to access and want to use for other purposes.

• Data portability should not undermine privacy: Privacy is an important principle in the context of data portability; while it is in certain cases important for service providers to allow access to user generated data, the principle should not be applied in a way that undermines the privacy and security of others. Data subject access should in most cases also not be required for data acquired from any source other than the subject itself.

• Data portability should not undermine incentives to innovate: Portability should not impair the ability of organizations to innovate and provide new services. When a service provider adds value to data provided by an individual, that value – which might come in the form of a supplemental set of information – should not be subject to any external data portability standards. This is needed to assure protection of the steward's legitimate business interests, including intellectual property rights. These incentives form the underpinnings of the U.S. patent, trademark, and copyright system which fosters innovation by granting innovators certain statutory exclusive rights in recognition of the risks taken and investments made by them in R&D. Relatedly, for data portability to support innovation it is important that it be reciprocated between service providers – portability reciprocity - otherwise incentives can be skewed and competition on the merits would be undermined.

• Data portability standards should be bottom-up and industry driven: In fast-moving technology markets, the IA supports a standard-setting model that is private sector-led, open, voluntary, consensus based, and nimble. While government has a role to play in encouraging industry standards and interoperability, the work to develop data portability standards facilitating interoperability between service providers should be driven by industry.

Conclusion

The Internet Association thanks the White House OSTP for the opportunity to comment on data portability policy. Our members share your interest and look forward to continued dialog with the OSTP on this and other issues.

Respondent 21

Lindsay Jager, Cerner Corporation

Essential for space management and exploration.

Cerner has long been committed to data portability and interoperability. We co-founded the CommonWell Health Alliance, a non-profit trade association dedicated to achieving cross-vendor interoperability that assures provider access to health data regardless of where care occurs. Our Associates have participated in JASON Task Force and Health IT Standards Committee work, focusing on the use of application programming interfaces (APIs) and Fast Healthcare Interoperability Resources (FHIR). We joined HL7 and industry partners to launch the Argonaut Project, aimed at accelerating the adoption of FHIR. Given our vast experience and future efforts in developing data portability and standards, we offer the

following suggestions to you: create standards from use cases, allow multi-stakeholder input, and require standards testing. These recommendations are outlined further below.

Benefits and Drawbacks of Data Portability:

The benefits of data portability are numerous and recognizable, including increased patient safety, health outcomes, and satisfaction. Productivity of healthcare providers increases and costs to patients and the health care system decline. Drawbacks that should be considered revolve around the creation and regulation of standards for data portability. If a standards-based interchange format is limited or unsuitable, a large amount of resources will be used to achieve an inadequate outcome. Friction between a government regulator and industry can lead to lost information and stifling of innovation. The decision to regulate standards should be made on a case-by-case basis, once a better understanding of market maturity, business affects, and operations are realized. In the case of overall data portability standards, the government should set a floor, not a ceiling, by which industry must comply.

Recommendation: Create Data Portability Standards from Use Cases

Best standards are developed out of usage experience, as opposed to being developed by a separate group or entity and enacted. In our opinion, it is more favorable and functional to standardize a common industry or business practice versus imposing a practice on industry. The focus should remain on existing business practices that are used broadly but where the market may not have settled on a standard of its own.

Recommendation: Allow Multi-Stakeholder Input

Industry should commit their own resources to regulatory discrepancies, while the government follows up with a steady and pre-determined timeline for full implementation expectations. Multi-stakeholder, industry lead, and voluntary input benefits the process greatly. An example of this in our industry is FHIR and use of APIs for exchanging data. The 2015 Edition Health IT Certification Criteria final rule, published by the Office of the National Coordinator for Health Information Technology (ONC), included a requirement for platforms to provide access to the Common Clinical Data Set via an API. Concurrently, HL7 and industry participants formed the Argonaut Project to accelerate the development of FHIR. Through this phased-in approach, key stakeholders are identifying gaps and ways to address standards while the government has made clear their intent and assumed timeline.
Recommendation: Require Testing of Data Portability Standards

Once standards have been agreed upon, the key to implementation is real world testing. Pilots are necessary and should be aggressive, including an aggregate of the population and the standard under consideration. If a standard is too difficult to test prior to full implementation, the risk of neglect or wrong doing outweighs the benefit of moving straight to implementation. Testing allows the flexibility and fluidity needed to make permanent changes prior to the final regulation being implemented.

Cerner believes health information should be portable and accessible across venues of care and to patients and their caregivers. Movement of information should be used to advance patient care between health care entities, regardless of the technological platform in place or location where care is provided. We are committed to open systems that enable collaboration across the health IT ecosystem, hastening the development of solutions that

improve patient outcomes and reduce health care costs. Cerner is appreciative of this opportunity to provide feedback and looks forward to working with the Office of Science and Technology Policy on next steps going forward.

Respondent 22

Aaron Seib, National Association for Trusted Exchange (NATE)

To Whom It May Concern:

Thank you for the opportunity to respond to this important request for information on behalf of the National Association for Trusted Exchange (NATE) and several of its members and allies. NATE (http://nate-trust.org) is a 501(c)(3) organization that brings the expertise of its membership and other stakeholders together to find common solutions that optimize the appropriate electronic exchange of health information for greater gains in technology adoption and improvement of patient outcomes. Emerging from the Western States Consortium, a pilot project supported by the U.S. Department of Health and Human Services' (HHS) Office of the National Coordinator for Health IT (ONC) that began in 2011, NATE was established as a not-for-profit organization in May 2013. Consistent with NATE's mission to address the legal, policy and technical barriers that inhibit health information exchange between data holders and healthcare consumers, NATE leads and participates in a number of ongoing and emerging projects focused on exchange via multiple modes of transport, including Direct secure messaging and APIs. NATE boasts organizational members of all types, from interested individuals to large organizations such as the U.S. Department of Veterans Affairs (VA).

We understand that the OSTP is most interested in responses related to the following topics:

1) the potential benefits and drawbacks of increased data portability;
2) the industries or types of data that would most benefit or be harmed by increased data portability;
3) the specific steps the Federal Government, private companies, associations, or others might take to encourage or require greater data portability (and the important benefits or drawbacks of each approach);
4) best practices in implementing data portability; and
5) any additional information related to data portability policy making, not requested above, that you believe OSTP should consider with respect to data portability.

With regard to questions (1) and (2) – the benefits and beneficiaries of increased data portability – the healthcare industry, and the patients and families served by it, could greatly benefit from increased data portability and technical interoperability. NATE is the only national nonprofit focused exclusively on reducing the barriers that inhibit a consumer's access to their health information. The driving force behind NATE's activities is an understanding that one of the foundational elements of HIPAA, the HITECH Act, and their implementing regulations is that individuals have a right to electronic access to their health information. Individuals now have an unprecedented opportunity to exercise their HIPAA right of access and become more engaged in their care, based on healthcare providers'

widespread adoption of certified electronic health record (EHR) technology and the Direct Project's secure exchange mechanism built into that technology. Furthermore, due to the availability of a wide variety of consumer-facing applications (CFAs), individuals have the ability to better receive, manage, and share their electronic protected health information (PHI). Secure electronic access to their PHI offers individuals a variety of benefits, including: (1) faster, less expensive access to health information; (2) receipt of the information in a form that is easier to review and manage; (3) increased ability to merge health records from multiple providers into one longitudinal record; (4) individual-centric health information exchange offers individuals an alternative means to ensure that their health information is transmitted from one healthcare provider to another in order to improve patient safety and care coordination; and (5) perhaps most important of all, the inherent patient safety benefits when the consumer and their proxy has the ability to identify and indicate corrections needed to their medical records to help ensure the highest quality care possible is delivered. In practice, however, individuals are finding that a great number of healthcare providers are not fully leveraging their EHR technology, either due to a lack of knowledge, vendor costs, or other barriers, to provide the consumer access to their protected health information as required by the HIPAA Privacy Rule (http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/).

NATE is committed to helping consumers access their health information via all appropriate means. NATE is a proud partner of the Get My Health Data Campaign (http://getmyhealthdata.org/), a collaborative effort among leading consumer organizations, healthcare experts, former policy makers and technology organizations working to enhance consumer access to digital health information. NATE's leadership is also committed to supporting Flip the Clinic's (http://fliptheclinic.org/flips/accessourdata/) goals of making health information accessible to consumers, empowering them to make their own decisions about when and with whom their data is shared. NATE provides focused recommendations and useful education about the technical options available to achieve the objectives of Flip the Clinic #55. NATE was honored to stand beside the Get My Health Data Campaign and Flip the Clinic when they were recognized by the White House as "Precision Medicine Champions of Change" (http://nate-trust.org/nate-videos/) on July 8, 2016.

With regard to question (3) – specific steps that might be taken to encourage or require greater data portability – one of best methods that the healthcare industry has developed thus far to encourage and enable data portability is through the development of Trust Communities. NATE has been operating its own Trust Bundles in production since 2012 (http://www.healthit.gov/buzz-blog/state-hie/western-states-consortium-pilot-direct-demonstrates-power-federalstate-coordination/) (If needed, see Appendix for an explanation of Trust Communities and Trust Bundles within the context of Direct Secure Messaging). Since that time, NATE has become the recognized leader in enabling HIPAA-covered entities to compliantly share protected health information with consumers. In 2014, NATE was entrusted with the administration of ONC's Blue Button Trust Bundle (using Direct secure messaging protocols) (http://nate-trust.org/wp-content/uploads/2014/08/NATE-BB+-FINAL-as-released.pdf). Under the governance of NATE, the Blue Button community continues to flourish. In 2015, NATE made the first release of the NATE Blue Button for Consumers (NBB4C) Trust Bundle (http://nate-trust.org/nbb4c-trust-bundle). The NBB4C provides a technical solution to establishing scalable trust among organizations using Direct secure messaging to exchange protected health information between HIPAA-covered entities and the consumers that they serve. The

NBB4C includes the trust anchors of multiple third party CFAs that have elected to adopt a common set of policies and practices that enable consumer mediated health information exchange while preserving personal privacy preferences. Working with a broad set of stakeholders through multiple task forces, crowdsourcing and a call for public comment, the process to determine the eligibility requirements that govern the NBB4C spanned two years and included multiple pilots funded by ONC and multiple State HIE programs. NATE undertook this effort in response to the needs expressed by all stakeholder types for the establishment of a national trust framework that reflects the distinct difference in regulatory requirements applicable to CFAs (that they are not subject to HIPAA, instead they are regulated by the Federal Trade Commission) and an ever-increasing demand on the part of consumers for secure access to this type of data via mobile and desktop applications. NATE is currently working to extend the utility of its trust community beyond Direct secure messaging to include other consumer-centric technologies, such as those that leverage APIs or other modes of exchange (NATE, in partnership with the Centers for Medicare and Medicaid Services' Blue Button API Team, will be leveraging FHIR-based resources and standard APIs to pilot the use of forward leaning technologies that allow a beneficiary to access their electronic health information from Medicare).

The NATE NBB4C is presently the only existing Trust Community that is specifically dedicated to maximizing opportunities for exchange between HIPAA-covered entities and the applications that consumers rely upon for managing their own data. One of the benefits of the NBB4C is the diversity of its participants and the services they offer through their applications. Because the NBB4C is a trust community that has agreed to a common set of security and privacy protections, HIPAA-covered entities that load the NBB4C into their trust stores can offer a wide range of trusted options for consumers looking to manage their health information for different purposes. One way that the Federal Government can specifically support greater healthcare data portability is to require that all HIPAA-covered entities subscribe to at least one consumer-focused trust bundle. When considering which trust bundles to subscribe to, it is important that HIPAA-covered entities are able to make local policy decisions that reflect their applicable policy requirements. However, NATE believes that it is also the patient's right to determine which CFA best serves their needs and that healthcare providers and/or their technology vendors should not be usurping this right by making their own determination about which consumer-facing applications should or should not be trusted (Additional information on this issue is available in the Appendix). Current guidance by the HHS Office of Civil Rights (OCR) supports this view, clarifying that once a patient's data is shared in the manner in which they request it, the provider sharing the data is no longer culpable in the event of a breach of that data.

Another way for the healthcare industry to encourage and enable greater data portability is by developing central portals through which common requests for information can be made and fulfilled. For example, NATE is currently working on developing a concept around the electronic submission of legal requests for medical records. Patients have a right under the HIPAA Privacy Rule to request copies of their personal health information from all of their providers, however this right of access typically hinges on the effective submission of a legal release of information form that is then acted upon by a medical records staffer. The person responsible for fulfilling the patient's request may not always be local to the provider's location. They may be part of a large Medical Records department or even an outsourced medical records warehouse. This can cause confusion for the patient and/or extra work for front office staff. Worse, if provider organizations are found by OCR to be preventing the patient from having access to their health information or otherwise acting as "information

blockers," they can be fined significant amounts. In order to simplify and streamline this process to make it easier for patients and providers alike, NATE suggests creating a single portal between which patients and Medical Records staff could communicate. On the patients' side, the portal could streamline the collection of a standard set of data most often included on a release of information form. On the providers' side, every registered Medical Records department would create an account that includes a Direct address. In registering, the Medical Records department would populate a profile with information about the providers that they serve, so that consumers could discover where their providers' records are managed and how best to access them. By registering with this medical records portal, the healthcare organization, and those entities that serve them, would have a single, secure queue from which they could establish a reliable process to ensure compliance with applicable law. At the center of this new flow of information between the patient and the Medical Records department would be the NATE NBB4C. Because the NBB4C aggregates consumer-facing applications, consumers could choose any one of a number of applications through which to obtain a secure Direct address, use a Direct message to make their request and receive their information.

With regard to question (4) – best practices in implementing data portability – this topic was discussed in great detail during the development of the NBB4C requirements. The community felt very strongly that allowing a patient to move their data from one application to another was a foundational element of this Trust Community. The NBB4C Onboarding Application (http://nate-trust.org/wp-content/uploads/2015/07/1-NBB4C-Onboarding-Application-3-d-1-REVISED-v3.7.pdf) specifically states that the applying "CFA shall ensure that an end-user is able to extract all of their structured data captured in the CFA and be able transport it to another location via Direct or another secure transport method." The reasoning for this requirement is clearly stated in the application: "The community being established by this bundle is intended to enable consumer choice and prevent vendor lock-in where the consumer's PHI is trapped in a CFA."

NBB4C participation criteria also address the question of what happens to a patient's data after they terminate their participation with the application. The criteria state that the "CFA shall ensure that an end-user is able to terminate their participation in the CFA and be able to request that their data be expunged in its entirety from the application and any data stores controlled by the CFA that may contain the end-user's PHI." The stated justification for this requirement is that "The community being established by this bundle is intended to ensure that the consumer has control over how its PHI is used, including how it is used after termination of the consumer's use of the application."

Note that the NBB4C calls for the portability of all structured data held by a CFA. From an electronic data portability policy perspective, and especially with regard to data stored in provider-controlled EHRs, NATE would recommend that this definition in fact be expanded. Patients currently have the right to receive an entire designated record set as defined by the HIPAA Privacy Rule, but most EHRs can only produce a part of that in a single action. Therefore, part of the workflow for the Medical Records department may require them to not only export a CCDA but to actually pull additional information from their internal data sources to respond to a consumer's request. This additional information could include unstructured data, radiology/pathology reports, OpenNotes, etc. Having all of the available patient data becomes especially important in legal malpractice cases in which patient records are requested by subpoena. Many patient portals are capable of providing this additional data but are prevented from doing so by internal policy controls.

To take this even one step further, NATE suggests that providing the patient or an authorized designee with a complete copy of their health information from an electronic record in a computable format may not even be enough to enable the patient to receive the most value from the receipt of their health information. Rather, we would recommend that the best data portability implementations would include both machine- and human-readable formats for those members of the population that may not have access to software that can render the machine-readable content in an end-user friendly manner.

Another key component to any successful data portability implementation is full transparency with regard to the use and storage of patient information. After requiring that NBB4C participants comply with all applicable state and federal laws and regulations, the next most important requirement for NBB4C participants is that they make clearly available their Notice of Privacy Practices. Specifically, "The CFA shall display their Notice of Privacy Practices (NPP) in an easily accessible location prior to sign up or use. [It must] include language on the application's data practices, including those areas addressed by the ONC Personal Health Record (PHR) Privacy Notice."

With regard to question (5) – additional information OSTP should consider in this policy-making area – NATE would suggest that a truly landmark action that could be taken in support of accurate data portability is for the Federal Government to finally resolve the "patient matching" issue. In addition to NATE's work around trust frameworks, NATE has been an active participant in community efforts to address the question of accurate matching between a patient and their information. In communities in which many people share the same name and often share other identifying characteristics as well, it can be a significant challenge to ensure that a patient's electronically stored information is accurate. NATE believes that work to improve algorithmic patient matching is important and supports the investigation of voluntary unique patient identifiers. A solution that is controlled by the consumer, allowing them to establish the correlation between their identifier and those identifiers that have been assigned to them by their numerous encounters with different parts of the healthcare system would not only simplify technical interoperability – it would literally save thousands of lives and reduce untold and unnecessary suffering and costs. One example might be to leverage the cryptographic key associated with the unique Direct address set up by the patient as a voluntary patient identifier.

We are optimistic about the maturation of the health ecosystem and support innovation with regard to next generation technologies. In fact, NATE is actively collaborating with numerous organizations to establish a new trust mechanism known as the TrustHarbor, which is designed to be the flexible enabling infrastructure that fosters broad adoption of API-based technologies across all types of use cases. Regardless of the technology used, it is critical that trusted mechanisms be made readily available to connect the applications used by patients to manage their health information with the clinical systems that hold that data.

On behalf of NATE, its members, and the undersigned, thank you for the opportunity to provide feedback on this request for information. If we can provide any additional information or clarification, please do not hesitate to contact NATE's CEO, Aaron Seib, at XXXXXXXXX.

Sincerely,

Aaron Seib, CEO
National Association for Trusted Exchange

Bart Carlson, CEO & Chief Patient Advocate
Azuba

Colin Wallis, Executive Director
Kantara Initiative

Brian Weiss, Founder
Carebox

MaryAnne Sterling, Co-Founder
Connected Health Resources

Kate Horle, Chief Operations Officer
CORHIO

Panha Chheng, CEO & Founder
Medyear

Bob Janacek, Co-Founder & CTO
DataMotion
Beth Davidson, State Health Information Technology Coordinator
Alaska Department of Health & Social Services

Elaine Scordakis, Assistant Director
California Office of Health Information Integrity

Christina Caraballo, Senior Healthcare Strategist
Get Real Health

Anand Prabhu, CEO/Founder
MediPortal

Tess Coody, Founder & CEO
Wellvana

Bettina Experton, MD, President & CEO
Humetrix

Linda Van Horn, President/CEO
iShare Medical

Paul Cartland, Owner
Total Link LLC

Respondent 23 (Appendix to Response 22)

Aaron Seib, National Association for Trusted Exchange (NATE)

In response to question (3) - the safety and control issues for AI.

APPENDIX: What is Direct Secure Messaging?
(Credit to Adam Greene of Davis Wright Tremaine)

To understand NATE's perspective, some background on the Direct Project may be helpful. Direct is a technical standard for exchanging health information between healthcare entities in a trusted network (http://www.healthit.gov/sites/default/files/directbasicsforprovidersqa_05092014.pdf). For Stages 2 and 3 certified EHR technology, EHR vendors are required to either (a) certify their transitions-of-care modules or complete EHR product offerings to include Direct to meet certification requirements, or (b) work with a third party to provide Direct services.

To oversimplify Direct secure messaging, it can be thought of as encrypted e-mails that incorporate digital certificates (known as Trust Anchors) to verify the identity and trustworthiness of the other party. The sender sends a Direct message to the sender's Health Information Service Provider (HISP). The sender's HISP then routes the message to the receiver's HISP. The receiver's HISP routes the message to the receiver.

For example, a physician's practice implements certified EHR technology. The EHR vendor either operates as the physician practice's HISP, or contracts with a third party to act as the physician practice's HISP. The physician is assigned a unique Direct address (e.g. PhysicianName@direct.EHRvendor.com). On the other end, a CFA vendor provides a unique Direct address (e.g. patient.name@direct.somephr.org) to each user of their product. The CFA either acts as a HISP or contracts with a third party to act as a HISP.

Under this system, every patient can readily download a third party application that supports Direct secure messaging (there are many from which to choose) and securely obtain a copy of his or her medical record summary from any healthcare provider who has implemented certified EHR technology. The primary obstacle, however, is that both the sender and receiver must have uploaded each other's Trust Anchors, otherwise the message will not be delivered. (http://wiki.directproject.org/Direct+Project+Security+Overview)

The Direct Project's Trust Anchors, Trust Communities, and Trust Bundles

As referenced above, a fundamental part of Direct secure messaging is the exchanging of certain digital certificates, known as Trust Anchors. The purpose of these Trust Anchors is that each party in a Direct Message knows the other party is who it claims (i.e. authentication) and also to find out information about its privacy and security policies.

For example, a hypothetical patient requests that her healthcare provider send her a copy of her medical record through Direct to patient.name@direct.somephr.org. If the healthcare

provider seeks to send the Direct message, then the healthcare provider's certified EHR technology will send the message containing the medical record to the EHR's HISP. The HISP maintains a "certificate store" (or "trust store") where a number of Trust Anchors (digital certificates) are maintained. The healthcare provider's HISP will contact a domain name server (DNS), the equivalent of an Internet phone book, which will respond that "somephr.org" is associated with a particular digital certificate. If the recipient's Trust Anchor is loaded into the HISP's trust store, then the transaction will proceed. If the recipient's Trust Anchor is not in the HISP's trust store, then the HISP will reject the healthcare provider's attempt to send the medical record to the patient's CFA.

The Direct Project promotes the creation of "Trust Communities" and corresponding "Trust Bundles." Trust Communities are formed by organizations voluntarily electing to follow a common set of policies and processes related to health information exchange. Examples of these policies include those that address identity proofing, certificate management, and privacy and security. (http://www.directtrust.org/trust-bundles/) Organizations such as NATE and DirectTrust create and maintain Trust Communities for users of Direct Secure Messaging (DirectTrust's Trust Community is focused on provider-to-provider exchange and NATE's Trust Community is focused on provider-to-patient exchange). Trust Communities' policies and procedures may differ significantly. For example, one Trust Community may require that its members go through an accreditation process with respect to their HIPAA compliance. Another Trust Community may rely on self-attestation with respect to privacy and security compliance, but may include requirements pertaining to state privacy laws or secondary use of data. NATE's Blue Button for Consumers (NBB4C) Trust Bundle is an example of a Trust Community.

For each Trust Community, there is a Trust Bundle, which is a collection of Trust Anchors (digital certificates) pertaining to members of the Trust Community. Through this process, a HISP can upload a single Trust Bundle, with knowledge that all Trust Anchors (digital certificates) correspond to a set of entities that meet certain minimum privacy and security requirements. An organization can choose to upload certain Trust Bundles but not others based on its own policy preferences. For example, a state-operated healthcare provider may choose to only accept Trust Bundles for Trust Communities that address compliance with both federal and state privacy and security laws. It is important to note that while Trust Bundles provide a means of uploading a large number of Trust Anchors at once, a HISP also can upload a single Trust Anchor.

The inclusion of a consumer-focused Trust Bundle, such as NATE's Blue Button for Consumers (NBB4C), is the stumbling block for widespread exchange between a provider and an individual's choice of third party health application, although it does not need to be. If the physician does not instruct its EHR vendor and/or HISP to include the Trust Anchor (or Trust Bundle) of the patient's CFA in the HISP's trust store, then the physician can attempt to send the patient's medical record summary to the Direct address of the patient, but the Direct message will not be delivered.

ONC provides the following guidance to healthcare providers on this issue:

ONCE I HAVE A DIRECT ADDRESS, WILL I BE ABLE TO EXCHANGE WITH ANY OTHER PROVIDER WITH A DIRECT ADDRESS?
Because Direct uses strong security to protect your communications (just like your trusted internet interactions with financial institutions, online retailers, and other secured

websites), certain steps may need to be taken to start exchanging information with another provider to ensure that they are a trusted connection. While much of the technical details of this will be handled by your EHR vendor, there are a few important points to note on establishing trust with other providers:
- Based on your system or the other provider's system, you may be required to indicate your wish to send and/or receive information from the other provider.
- Depending on the EHR and/or HISP you and the receiving provider are using, you need assistance from your vendor to establish this trusted relationship
- Some work between the two vendors may be required in order to communicate. If you have questions about communicating with another provider, check with your EHR vendor or Direct HISP as a first point of contact.

The problem is that, in practice, healthcare providers are not asking their EHR vendors or HISPs to be able to communicate with patients through third party applications. Accordingly, when a patient with a CFA-provided Direct address requests his or her records in a convenient, inexpensive, and readily producible manner, the request is denied or does not work. This may occur for any number of reasons. The healthcare provider may be confused and not know the step it needs to take. The healthcare provider may mistakenly believe that HIPAA does not permit them to exchange protected health information directly with a third party application at the individual's request. The healthcare provider may believe that it is inappropriate to exchange protected health information with an entity, such as a CFA, that is not subject to HIPAA. The healthcare provider may interpret that the requested form and format is not "readily producible" since the healthcare provider would need to take some action (e.g. contacting the EHR vendor or HISP) to enable the exchange. Or the healthcare provider simply may not want to go through the effort of contacting the EHR vendor or HISP and requesting the exchange of the relevant Trust Anchors (digital certificates). Whatever the reason, the result is the same – one of the most convenient ways for the patient to receive his or her information and become better engaged in a secure manner is denied.

The NATE NBB4C includes privacy and security requirements above the minimum legal requirements for participating CFAs. A healthcare provider need not initiate trust relationships with the third party application of the patient's choice on a one-off basis, but can instead take the single step of requesting that its EHR vendor or HISP permit exchange with all members of the NBB4C. This will immediately facilitate the healthcare provider being able to send Direct messages to a variety of PHR applications, all of which have agreed to meet certain privacy and security requirements. Despite the ease of this step, healthcare providers and their HISPs are not taking this action and instead are denying patients access to their electronic medical records through Direct secure messaging.
Trust Anchors and the HIPAA Right of Access

The use of Trust Anchors is invaluable in the exchange of health information between parties. Where a physician has discretion as to whether to provide protected health information to a recipient, the Trust Anchors model provides an easy and scalable means for the physician to know that the protected health information is going to the correct recipient and to have a level of comfort regarding that recipient's privacy and security safeguards. Otherwise, each physician would need to take steps to confirm the identity of each recipient, and may also wish to look at the recipient's privacy and security practices. But the Trust Anchor model should not be used as an impediment to an individual exercising his or her right of access.

While HIPAA generally provides a covered entity with discretion as to whether to disclose protected health information, a covered entity is required to disclose protected health information maintained in a designated record set to an individual upon the individual's request (45 C.F.R. §§ 164.502(a)(2)(i) and 164.524). A covered entity cannot refuse to provide an individual with a copy of the individual's designated record set because the individual does not maintain sufficient privacy and security practices.

The HITECH Act and its corresponding regulations clarified that an individual can require that the covered entity send an electronic copy of the designated record set to a designated third party (42 U.S.C. § 17935(e); 45 C.F.R. § 164.524(c)(3)(ii)). The covered entity must provide the electronic copy in the form and format requested by the individual, if it is readily producible in such form and format (45 C.F.R. § 164.524(c)(2)(i)). Nothing in HIPAA permits the covered entity to deny the individual's request because the designated recipient does not have sufficient privacy and security policies in place.

Accordingly, when a patient requests that a HIPAA-covered healthcare provider that has implemented certified EHR technology transmit protected health information in a designated record set to the patient's choice of CFA via Direct secure messaging, the healthcare provider is required to do so (An exception would be if a healthcare provider has a valid basis for denying the request, such as where the access is reasonably likely to endanger the life or physical safety of the patient or another person). The healthcare provider must verify the patient's identity (45 C.F.R. § 164.514(h)), but the healthcare provider may not claim that the requested form or format is not feasible, since the certified EHR technology readily allows for the exchange. The healthcare provider may not refuse to contact the EHR vendor or HISP and request that the CFA's Trust Anchor be added. The healthcare provider may not claim that it does not have a sufficient basis for trusting the third party application of the patient's choice, because it is not the healthcare provider's place to question the privacy and security practices, or even the identity verification, of the patient's designated recipient.

Make no mistake, we are not advocating for poor privacy and security practices for third party applications. We firmly believe that CFAs should be transparent in their privacy and security practices, such as through the ONC PHR Model Privacy Notice, and should not use health information for any purposes without the patient's knowledge. But it falls to the patient to decide whether he/she wants to trust his or her health information to a particular CFA. No healthcare provider should be permitted to deny an individual's request for access based on the provider's unwillingness to request the upload of a CFA's Trust Anchor to the HISP's trust store.

- Unknown Unknowns. Given that a superintelligence is capable of inventing dangers we are not capable of predicting, there is room for something much worse but which at this time has not been considered.

Respondent 23

Jerome Glenn, The Millennium Project

The Millennium Project conducted 4 surveys on Future Work/Technology 2050 with over 450 AI and related experts from over 45 countries to produce three global scenarios that connect today to 2050 with cause and effect links that illustract decsions. These are beging given to national planning workshops around the world and are avail for you at http://www.millennium-project.org/millennium/Work-Tech-2050-Scenarios.pdf