Data Protection and Credit Information Sharing

A PERC White Paper

Patrick Walker

PERC

November 2017

Introduction

Societies and economies are increasingly becoming data driven. The growing influence of social media, online shopping, search engines, online services, Big Data, biometrics, artificial intelligence, machine learning and the emergence of the so-called Internet of Things (IoTs) are spawning new, rapidly growing sectors and companies and disrupting the old. This not only raises the need for certain data protection rules but also raises the need to get data protection rules *right*.

Globally, regulators, policymakers, and thought-leaders are grappling to define basic aspects of this new landscape. For instance, what exactly *is* Big Data. After all, large data sets have been collected for decades now. Data aggregators, such as credit bureaus, have existed since the 1800s. And data on customers have been collected for centuries. Some of the oldest surviving written records are of economic transactions.

For much of this data gathering history, data protection rules arose out of need. Some rules were ad hoc, some were company policy specific, some were activity specific, or some were sector specific. For instance, consider centuries old Swiss banking privacy rules or century plus old privacy rules regarding US (individual level record) Census data.

As a result of growing databases, both private and public, the last several decades has seen the introduction of many sector specific data rules, including the Fair Credit Reporting Act (FCRA) in the credit-reporting sector in the US. The growth in databases and the possibilities of data exchanges over the past few decades have, of course, been the result of IT developments. Nonetheless, there is now very strong interest in the US and globally regarding data protection rules.

What makes data different *now*?

Obviously some tipping point has been reached. It is safe to assume that the underlying policy issues involving data and data protection will not fade. Attempts to measure the annual increase in the volume of data produced find that it is growing at an exponential rate.[1] That is, this interest and perceived need is no fad. But rapid change also means that it is difficult to predict what the pressing data protection issues will be (and rules needed) in 20, 30 or 50 years.

[1] For instance see https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm or https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html

General Approaches to Data Protection in Credit Information Sharing

On a very high level, one could classify data protection rules as falling into two general approaches. The first approach is a "siloed," sectorial, or need-specific approach. This can generally describe the US's approach.[2]

The advantage of this approach is that rules and guidelines can be tailored to specific needs, and industries, and activities. This may be most likely to produce appropriate rules for *specific* activities. However, there are instances in which data are collected and used outside of the silos, such as when data is collected on consumers regarding retail business transactions and used for "ungoverned" purposes. There may also be ambiguity regarding whether an activity is within a silo or it may be the case that an activity is within multiple silos with differing rules.[3] With the increasing importance (and collection and use) of data in virtually all sectors, this will likely grow as an issue.

Another data protection approach is an omnibus or comprehensive approach. This can generally describe the European Union's (EU's) approach to data protection. The General Data Protection Regulation ("GDPR" officially Regulation (EU) 2016/679) takes a holistic approach to governing the collection, storage, use, transmission, and sale of data.[4] The GDPR also regulates transborder data flows. Designed to strengthen data protections and empower individual data subjects, the GDPR replaces the EU's Data Protection Directive (Directive 95/46/EC). Both the GDPR and its' predecessor, the Data Protection Directive, cover data collection, protection and exchange generally, across sectors and activities. This may be an advantage when the aim of the directive was to corral multiple national data rules into a more unified framework. A potential downside to this approach is that it can be seen as being a "one-size-fits-all" approach that is not properly gauged to specific needs.[5]

---

[2] In the US, for instance, the FCRA covers credit bureau data, HIPAA covers health data, COPPA for websites that collect data on children, The Privacy Act covers government data, and so on. Each of these may govern individual/data subject rights, how data may be used, what data may be collected, how it can be shared, and data security.

[3] The "ad hoc" approach likely took root in the US since rules were built up over time addressing specific concerns. And given the weight attached to freedom of speech, it may be difficult to craft a single set of rules that would cover all data/information collection and flows (for example, collecting public record information or information from newspapers about data subjects).

[4] "Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC." (General Data Protection Regulation). L119, 4/5/2016, pgs. 1-88.

[5] In these simplistic descriptions, the EU is like a city with a single speed limit, no nuance in the rules. Whereas, the US is like a city that has particular, well thought out speed limits on some sections of its roads and no posted speed limits on remaining sections. And as with data protection rules and the explosion of data, as traffic grows in each city the flaws in either approach will become costlier and ever more clear.

The reality of data protection governance in the US and the EU appears to be more flexible and reflective of pragmatism than might be assumed.

Firstly, in the US, the silos covered by particular laws or agency powers can be broad. For instance, the newly created CFPB is a federal agency that oversees consumer reporting agencies (CRAs), banks, credit card issuer and other entities. Privacy and data protection are part of its scope of coverage.[6] And FCRA case has been brought against an online (people) search engine, Spokeo, in addition to earlier FTC action against Spokeo, also using the FCRA.[7] And the FTC, an agency with very broad powers, covering virtually all national commerce, oversees many consumer data privacy and security rules (such as COPPA) and enforces the U.S.-EU Safe Harbor Framework provide, in which companies certify that they comply with the seven privacy principles required to meet the EU's adequacy standard.[8] The FTC is also a watchdog agency for "Unfair or Deceptive Acts or Practices," which is one aspect that helps to ensure that US regulators have comprehensive authority.[9] This authority enables the FTC to make sure companies are living up to their own data security, data protections, and data transfer statements made to consumers. The FTC has also moved further beyond rule-specific powers or enforcing statements made to consumers to more general enforcement of data security.[10] Under its "Unfair Practices" authority, the FTC has assumed regulatory authority over data security.[11]

Going beyond data security, the FTC also has proposed a more ambitious data privacy framework.[12] The proposed framework covers, among other issues, data retention, data collection, data security, data accuracy, consumer interactions, transparency, consent or choices, notices and data that, while not specifically

---

[6] For instance see an amendment to annual privacy notice requirements by the CFPB, http://files.consumerfinance.gov/f/201405_cfpb_annual-privacy-notice-proposal.pdf

[7] See https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed and https://www.law360.com/articles/954349/9th-circ-says-fcra-claims-meet-standing-bar-in-spokeo-row

[8] See FTC, "Federal Trade Commission 2014 Privacy and Data Security Update". Accessed at https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

[9] See FTC, "A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority." Revised July 2008. Accessed at https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority

[10] See the complaint and a supplemental memorandum of the FTC available on the FTC's website, https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf and https://www.ftc.gov/system/files/documents/cases/150327wyndhamsuppbrief.pdf.

[11] In a suit against Wyndham Worldwide, the FTC has alleged that the company's data security was inadequate. The FTC argued, "the FTC has acted under its procedures to establish that unreasonable data security practices that harm consumers are indeed unfair within the meaning of Section 5. First, the LabMD Order directly states the Commission's considered determination that inadequate data security can be an unfair practice."

[12] FTC, "Protecting Consumer Privacy in an Era of Rapid Change." March 2012. Accessed at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

personally identifiable, could become so if combined with other data elements.[13] This aspect is particularly relevant in the era of Big Data.

The EU, looking to harmonize national laws and frameworks, begins with a unified, omnibus directive, Directive 95/46/EC. This covers data collection, data retention, consumer/data subject rights, data accuracy, among other issues. This has been replaced with the GDPR which broadens the scope of regulation designed to protect individuals. Unlike the Data Protection Directive, the GDPR does not require EU member states to pass binding legislation and simply takes direct effect.

The FTC proposed general framework, the OECD's Guidelines on data protection and privacy[14], and the EU's GDPR and Data Protection Directive are general in nature and do not specify details of which data elements can be collected, in which industries, and how long then need to be retained. Instead, guidance is usually expressed in terms of what is necessary for the business activity. For instance, an EU guide notes that "Personal data can only be processed" in a number of cases including when,

> "The data subject has unambiguously given his or her consent," or "Data processing is necessary for the performance of a contract involving the data subject or in order to enter into a contract requested by the data subject, e.g. processing of data for billing purposes or processing of data relating to an applicant for a job or for a loan;"[15]

It also notes that there needs to be a reasonable balance struck between privacy and business interest and needs, for instance, it states,

> "Finally data can be processed whenever the controller or a third party has a legitimate interest in doing so. However, this interest cannot override the interests or fundamental rights of the data subject, particularly the right to privacy. This provision establishes the need to strike a reasonable balance, in practice, between the business interest of the data controllers and the privacy of data subjects. This balance is first evaluated by the data controllers under the supervision of the data protection authorities, although if required, the courts have the final decision."

---

[13] The FTC is proposing that the framework cover all companies other than those that handle just a limited amount of non-sensitive data that is not shared with third parties.

[14] OECD. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", accessed at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#scope

[15] See http://ec.europa.eu/justice/policies/privacy/docs/guide/guide-ukingdom_en.pdf for the guide and http://ec.europa.eu/archives/ISPO/legal/en/dataprot/directiv/directiv.html for the directive.

The guide also notes that various reasonable exceptions can be made by EU member states and that supervisory authorities in the member states have the responsibility "to monitor the application of the Directive." Given how recently the GDPR has taken effect, it remains unclear whether and to what extent there will be flexibility with the interpretation and implementation of this new omnibus data protection law.

Using the general directive as a precedent, it thus falls on member states laws, member state supervisory authorities, courts, and / or other EU rules and guidance to determine how the directive is applied to specific industries and activities. While the GDPR is a single set of regulations to be applied across the EU, there are, nonetheless, variance and exceptions permitted to account for member states law and needs. And the principles of the GDPR will be applied differently across various functions and within different sectors. For example, specifics of what constitutes appropriate data collection and retention for one purpose (such as credit reporting) will be separate and distinct from rules for others.

Therefore, the omnibus approach of the EU is not really an inflexible "one-size-fits-all" approach. And the US's sectorial approach does not leave consumer data mostly unregulated. Despite seemingly very different approaches to data protection, these two regimes may, ultimately, become more similar in effective application than distinct.

Another way to look at this is the US has started with well-defined sectorial data protections and now appears to be moving to fill in the gaps with broader, more general standards as it becomes apparent that the growth of data is exploding in all facets of society. The EU is responding to the exploding growth of data by pursuing a more general data protection framework, that, with sufficient flexibility, will bend to the reality of different activities with exceptions and differences in specific rules. It would not be surprising if both the EU and US ended up with similar frameworks, ones with both general and activity/sector specific rules. While neither may characterize their frameworks as such, that is how they may end up in reality.

The exponential growth of data will likely drive most societies to create some form of underlying general data rules and protections. On the other hand, the reality that different specific rules and protections are needed for different activities (government data vs. credit reporting data vs. health data vs. social media, etc) means that activity or sector specific rules are also necessary.

Data Protections and Credit Reporting

Credit reporting is an activity that typically has applied to it specific data protection rules. This activity and its governing rules often pre-date not only Big Data but electronic databases. There are compelling reasons for credit reporting to have specific rules. First, there are vital consumer, national, and business economic interests from enabling robust credit data sharing. Second, the very logic of credit reporting is inconsistent with consumers exercising complete control over what

data is shared, largely because of the interests of consumers individually and collectively. The more complete that consumer risk profiles can be produced through the broader sharing of data, the easier it is for lenders to make sure that particular consumers can afford loans and not become overindebted. Additionally, the easier it is for oversight agencies to hold lenders accountable for overlending. For lenders to effectively measure whether consumers can afford a loan and for regulators to see if lenders are overlending, negative data (such as very late payments, charge offs, etc.) is often not enough. Overindebtedness crises, such as in Hong Kong in the late 1990s, showed that negative data was insufficient, as debt levels rose with consumers taking on new loans to service older ones. This is because negative data often shows that consumers are not late in making payments, but, at the same time, lenders do not see rising outstanding balances as consumers enter an unsustainable borrowing cycle.[16]

Credit reporting data are useful to consumers/applicants because they are *not* controlled by the consumers/applicants. That is the very point of credit reporting. It is independent, third-party data that the data subjects (consumers/applicants) can not easily game. Otherwise, lenders could simply *ask* consumers on credit applications, have you ever defaulted, ever been late on a credit payment, how indebted are you currently, and do you pay your bills on time and simply take their word for it.

Additionally, the secondary market and overall financial system and national economy, need lending products associated with transparent, independent, useful data to gauge risk and capacity as much as is economically possible. The financial crisis in the US began with a subprime mortgage crisis in which many loans were originated and sold based poor underwriting and misaligned incentives. Part of the poor underwriting were loans that were based on a consumer's stated, unverified, income. These were often called low documentation loans since they did not rely on extensive third party, independent verifications of consumer income and assets.[17] These loans were found to be rife with income falsifications and suffered much higher delinquency rates. The policy response was to mandate that mortgage loans utilize, third-party, independent verification of borrower income or assets.[18] Legislation requiring third-party verification of total outstanding debt levels, credit risk scores, past repayment histories, and available credit was not needed since credit bureaus already made such comprehensive information inexpensively available to lenders resulting in its near universal use.

---

[16] While less talked about in the literature, comprehensive, full-file reporting can increase the transparency of underwriting and limit "creditor moral hazard", where lenders overlend in the pre-crisis stage, and shift the burden to the public in the crisis. Jean Tirole, *Financial Crises, Liquidity, and the International Monetary System*. p. 42

[17] Wei Jiang, Ashlyn Nelson, and Edward Vytlacil. "Liar's Loan? Effects of Origination Channel and Information Falsification on Mortgage Delinquency ", April 2011. Accessed at: http://www8.gsb.columbia.edu/sites/financialstudies/files/files/liars_loan.pdf

[18] Dodd-Frank Wall Street Reform and Consumer Protection Act. Accessed at: http://www.gpo.gov/fdsys/pkg/PLAW-111publ203/pdf/PLAW-111publ203.pdf

It is obvious why a financial system and society, where possible, should base consumer loans on third-party, independent data, and not simply take applicants, and even originators, at their word (moral hazard, adverse selection, misaligned incentives). Moreover, lenders, in conditions when the economy is flush with liquidity, have interests in making as many loans as possible, and will relax underwriting standards. The availability of a comprehensive, full-file data system can help regulators encourage more rigorous underwriting standards. For these basic reasons credit reporting is not typically carried out at the discretion of the consumer or even the lender. Similarly, governments maintain tax databases and other independent databases on individuals and companies and do not give much choice to data subjects as to what is collected and maintained.

In exchange for the loss of the practical ability to "edit" or control what goes in to their credit reports, and the fact that credit reports are consequential, consumers have been given extensive rights to review their credit reports, dispute inaccuracies, and determine who sees them. The credit bureaus that house these reports (data) are typically highly regulated and supervised.

That is, governments typically lower barriers (or don't raise barriers) and encourage credit data to be gathered but then grant the consumer/data subject rights to verify credit data accuracy and rights on who sees the data.

These "lowered" barriers between banks and credit bureaus and "raised" barriers between credit bureaus and end users allows: (1) data to be gathered that is not "edited" by consumers so as to more accurately reflect credit risk and capacity; but, (2) grants ultimate control of who can access this data to consumers. ***This empowers the consumer to share unbiased information on their credit profile when they wish.*** It thereby reconciles the needs of the system to share the data for financial stability, safety and soundness, on the one hand, with consumer privacy and consumer data protections on the other.

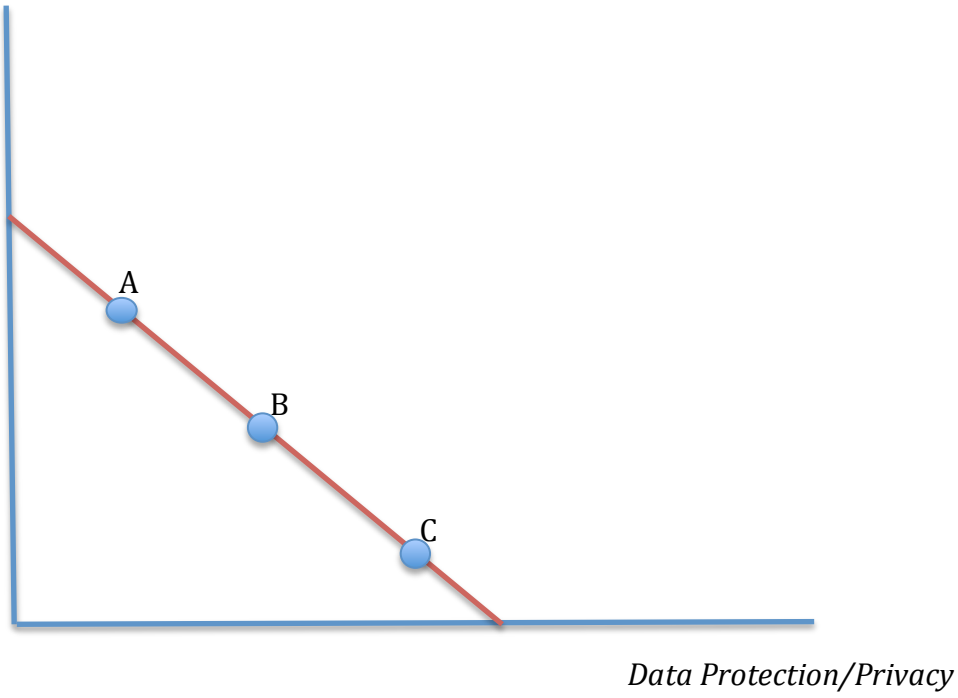
This maintains the integrity of credit data, producing a transparency with respect to a consumer's unbiased past and present credit situation. In turn, this produces better lending, improved consumer protection from overindebtedness, increased banking competition, and increased and fairer access to credit, without a practical loss of data control by consumers.

Data protections that erect unduly burdensome barriers to the movement of consumer data from one institution to another necessarily impacts credit data sharing. But how credit sharing might be impacted by this very much depends on the *details* of the data protections and how they are implemented.

Tradeoffs Between Data Protection and Information Sharing?

When the issues of data protection and information sharing (or other activities in which data is exchanged and used) are discussed it is often noted that there is a tradeoff between the two. This is usually taken as a given. The symbol of a scale is often used as a way to symbolize the need to balance data protection and information sharing. The danger with the simple notion of a tradeoff or a scale is that it misses key parts of the issues involved and can be misleading.

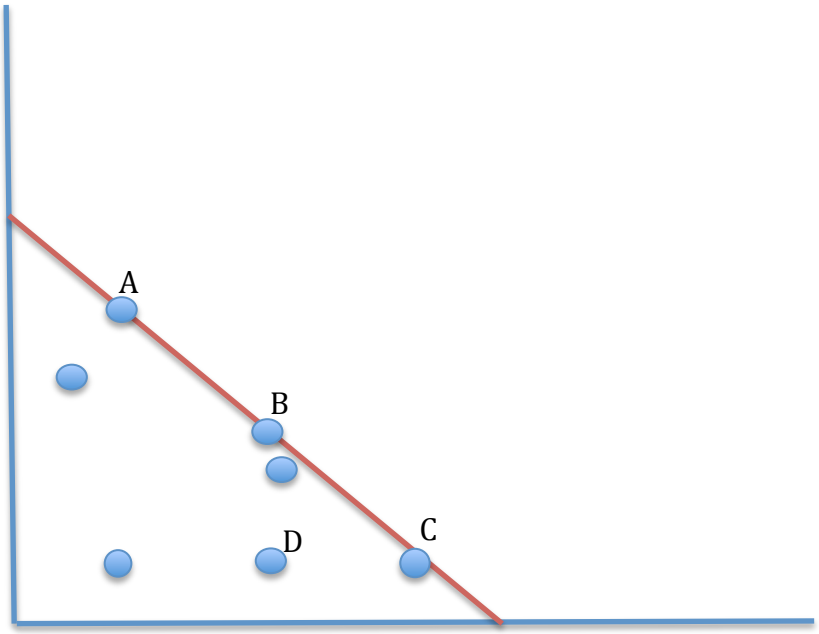
For instance, the notion of a scale or a simple tradeoff can be seen as policymakers choosing between points A, B, C with different sets of policies and rules.



In this view of reality, social norms and preferences help guide the choice between A, B, and C. Very high-level, general discussions of privacy and the values of information flows can take people down this path.

But this ignores the fundamental reality that most policies are not optimal for a given industry, sector, or specific activity. That is, there are many, many more interior points. Small details of rules can be hugely important as well as the realities "on the ground" of specific industries and activities. If rules do not take these realities into account, interior points, deep interior points should be expected.

Information Sharing /
Economic Benefits of Data



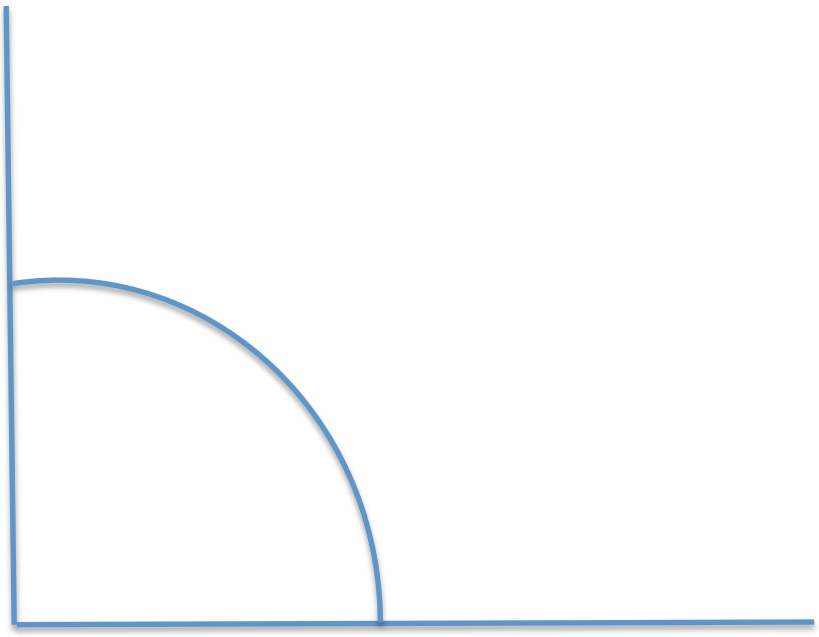
Data Protection/Privacy

So, policies/rules that result in D can occur. These are poorly structured rules that produce a decent degree of data protection and privacy by at an *unnecessarily* high cost to the benefits of data exchanges. In this context, what is perhaps more important than how much information sharing one is willing to trade for data protection on the frontier is simply choosing appropriate, well tailored rules/policies to get you *to* or at least *near* the frontier.

The other issue is then the shape of the frontier.

It is likely that if one is on the frontier with a maximum value of data flows, that if done optimally, just a very little data sharing can initially be given up to gain a lot of privacy, and vice versa. So, the shape may be more like the following.

Information Sharing /
Economic Benefits of Data



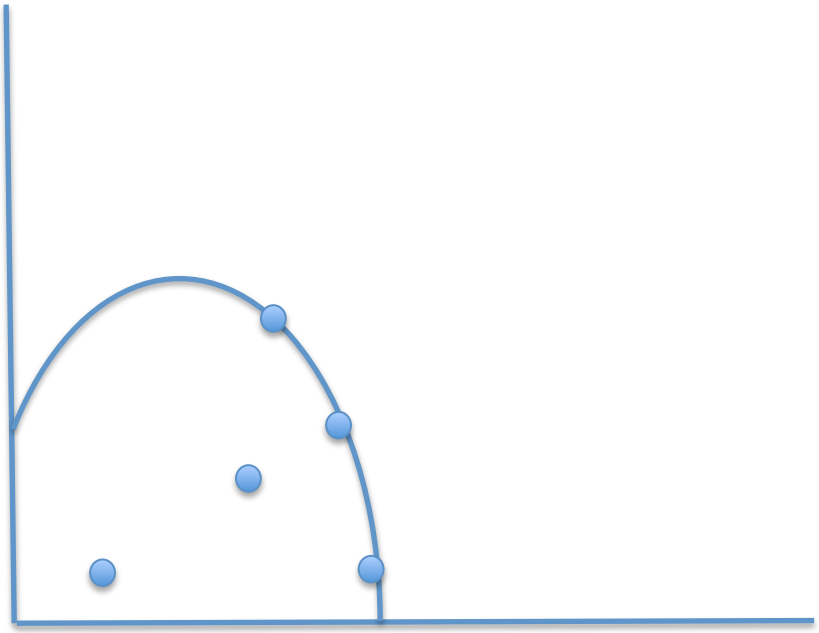
Data Protection/Privacy

So, in this case, a few minor tweaks, can gain a good deal of Data Protection with only very little loss to the value of data flows (such as using encryption).

Another interesting possibility, is that the overall level of Data Protection/Privacy may, of course, impact trust in data sharing and the value in data flows. So, very low levels of Data Protection means very little overall trust, which, in turn, reduces data flows.

This notion produces the following frontier.

Information Sharing /
Economic Benefits of Data



Data Protection/Privacy

Now the whole notion of a simple tradeoff is thrown out the window. Here it is possible to choose a set of policies/rules that produces both a good deal of Data Protection *with* a good deal of valuable data flows. Both can be achieved if the details of the rules/policy are structured properly.

Summary

Societies around the world are grappling with the thorny issue of creating appropriate data rules and protections. The false starting point is whether a sectorial/activity based approach or a general/omnibus approach is preferred. What appears to be developing in the US and EU is a hybrid approach, though each from different starting points. While a pure sectorial approach may seem well tailored to the specific needs of particular activities and types of data, the absence of overall data rules and protections means gaps between sectors might be ungoverned and activities that may fall into multiple sectors could have multiple sets of rules and protections.

On the other hand, while a single set of data protection rules covering all sectors may seem like the ideal, logical, and "beautiful" approach, assuming data on a person is data on a person no matter what, the reality of specific needs for particular activities/sectors suggests otherwise. Should the specifics of consents, ownership, rights and rules really be the same for data shared with the government, with health providers for medical research, with data exchanged in credit reporting, information published in newspapers, information collected by banks, information put on Facebook? Of course not. Whatever benefits are derived from such strict consistency would be overwhelmed by the very high costs of the inflexibility. As such, omnibus rules (like the EU's) often allow for exceptions, exemptions, and flexible interpretation of general rules, and flexibility of how specific rules are implemented, etc. This results in, from a practical perspective, sets of sector/activity specific rules. The more flexibility an omnibus framework has (to a reasonable extent), the better. This held for the general EU data protection directive from 1995 until this year, and will be so with the GPDR moving forward.

What really matters, whether the overall data protection framework is considered sectorial or omnibus, are the specific rules implemented in particular sectors. The devil is in the details. As data protections evolve in the US and the GPDR is enacted and evolves in the EU, close attention should be paid to not only the privacy and data protections aims of the rules but also to how well they incorporate common sense, are appropriately flexible, are proportionate, adhere to the differing needs and realities of different data uses and activities, and don't *unnecessarily* inhibit information flows and data processing due to poorly constructed specific rules and regulations.

As with the case of credit reporting, well-tailored data protection rules can enable both meaningful consumer data protections *without* unduly inhibiting useful data exchanges and data dependent activities.