Date Protection: Is the law doing enough?

-Rishabh Jogani[1]

Abstract

In an age of increasing technological development, rampant invasion of privacy and the creation of a market place that trades in data about people; what has the law done to protect the rights of individuals?

Introduction

"Advances in the technology of surveillance and the recording, storage, and retrieval of information have made it either impossible or extremely costly for individuals to protect the same level of privacy that was once enjoyed.[2]"

In as early as 1890, Warren and Brandeis in their article appearing in the Harvard Law Review, argued that, "the intensity and complexity of life, attendant uponadvancing civilisation, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, sothat solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[3]"

The commercial dealing in private information is a violation of the right of an individual to his own privacy and States are required to take necessary steps, through appropriate legislation to protect individuals and their privacy. However, the question really is whether nations have really enacted or are in the process of enacting laws, which are capable of dealing with these issues and to what extent would the law protect individuals as well as corporates. The focus of this essay shall be the European Union and the United States of America and an analysis of the application of these laws.

---

[1]Rishabh Jogani, Advocate Bombay High Court

[2] R Gavison, 'Privacy and the Limits of Law' [1980] 89 Yale Law Journal[421], [465]

[3] 'The Right to Privacy', 4 Harvard L.R. 193

An application developer who collects and aggregates personal data, behavioural data and location data for his/her own purposes and in order to sell this data to third parties will be the starting point of the legal discussion, and the analysis in this essay shall be made based on his/her position in law.

Data Protection in the United States

Considering that, "…in the U.S., there is no single, comprehensive federal (national) law regulating the collection and use of personal data. Instead, the U.S. has a patchwork system of federal and state laws, and regulations that overlap, dovetail and may contradict one another.[4]"

There are also many guidelines, which have been developed by governmental agencies and industry groups that are which although not legally enforceable are still adhered to as part of self-regulatory efforts of developers and are considered the best practices in the market.

It has been argued that, "The proliferation of security breaches in recent years has led to an expansion of this patchwork system of privacy laws, regulations and guidelines which is becoming one of the fastest growing areas of legal regulation. The combination of an increase in interstate and cross-border data flow, together with the increased enactment of data protection related statutes heightens the risk of privacy violations and creates a significant challenge for a data controller to negotiate the onerous and often inconsistent requirements for each state, when operating at a national level.[5]" What is important to consider however is that the Federal Trade Commission (FTC) of the United States through numerous measures[6] has provided for data protection.

In addition certain privacy bills have been introduced in the U.S. Legislature which include:

---

[4] Practical Law, <http://uk.practicallaw.com/6-502-0467#a89631>

[5] Practical Law, <http://uk.practicallaw.com/6-502-0467#a89631>

[6] *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers* .

1. The Do Not Track Me Online Act

The Do Not Track Me Online Act[7], "would authorise the FTC to establish standards for an online opt-out mechanism aimed at providing internet users with a method to prevent the collection and use of certain personal information, including personal identifiers, and online search and browsing habits. The bill would also require covered entities (that is, entities which are engaged in interstate commerce and collect or store online data containing personal information), to disclose their information collection practices, including the names of those to whom the entities disclose this information. The bill would authorise the FTC to develop rules requiring covered entities to provide consumers with access to their data.[8]" It has been suggested that the proposed legislation will mandate the Commission to promulgate regulations to establish standards for the establishment of a Do Not Track regime.[9]

Section 3(a) of the proposed legislation directs the FTC to, "…establish standards for the required use of an online opt-out mechanism to allow a consumer to effectively and easily prohibit the collection or use of any covered information and to require a covered entity to respect the choice of such consumer to opt-out of such collection or use.[10]" This proposed legislation leaves it to the FTC to take measures and create regulations that are necessary in order to enforce the provisions of the law. An app developer in case the legislation is enacted will be forced to create a mechanism for the deletion of personal data, which is collected from users.

Although this legislation aims to ensure online privacy it suffers from the inherent fault of not doing enough to protect the internet service provider or data collectors who provide free services to users but in exchange subject them to advertisements. Howard Beales cautions about these market repercussions of this enactment and says

---

[7]Do Not Track Me Online Act (draft), <http://www.gpo.gov/fdsys/pkg/BILLS-112hr654ih/pdf/BILLS-112hr654ih.pdf>

[8] Practical Law, <http://uk.practicallaw.com/6-502-0467#a89631>

[9] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, FTC Report.
<http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>

[10] Section 3(a), Do Not Track Me Online Act (draft), 2011 H.R. 654.

that, "If advertising is to remain the primary means of financing Internet content, then advertising rates will be a critical determinant of the kind and quality of Internet content available. Unless publishers can effectively capture some of the value they create for viewers, they will not be able to provide as much content, or content of the same quality as viewers have come to expect.[11]"

It can be argued that, although consumers would prefer not having their data collected by websites or applications, they would be unable to object if the collection of data is the only means of using the application for free or without paying large sums of money to the developer. In addition, this proposed legislation would also cause practical difficulty for the app. developers who provide services for free but will have no incentive to develop or create applications because most business models rely on data transfer as a means of revenue, blocking such a means of revenue would spell doom for the industry as a whole.

2. Application Privacy, Protection, and Security Act of 2013

Introduced in May 2013, thelawaims to provide for greater transparency in and user control over the treatment of data collected by mobile applications and to enhance the security of such data.[12]The key features of this legislation are:

a) Consent, Transparency and User Control

Section 2 (a) of the proposed legislation requires the developer of a mobile application which collects personal data about a user of the application, to "(A) provide the user with notice of the terms and conditions governing the collection, use, storage, and sharing of the personal data; and (B) obtain the consent of the user to such terms and conditions.[13]" This provision would require a developer to ensure that it gives a user a chance to opt-in for data storage and collection by requiring the user to consent to the terms and conditions authorising the collection and storage of data.

---

[11] Howard Beales, The value of Behavioral targeting.
<http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf>
[12] H.R. 1913: Application Privacy, Protection, and Security Act of 2013 (draft).
<https://www.govtrack.us/congress/bills/113/hr1913/text>
[13] Section 2 (a), Application Privacy, Protection, and Security Act of 2013 (draft)

An obligation is also imposed to inform the user about exactly what data will be collected, for what purpose the data will be used and where the data will be given to third parties, details of those parties. Considering that most applications always require acceptance of general terms and conditions prior to use, the effect of this provision may not be extra ordinary.

b) Withdrawal of Consent & the Right to be Forgotten:

Section 2 (b) provides for a situation of withdrawal of consent and mandates that, "The developer of a mobile application shall - (1) provide a user of the application with a means of— (A) notifying the developer that the user intends to stop using the application; and (B) requesting the developer - (i) to refrain from any further collection of personal data through the application; and (ii) at the option of the user, either— (I) to the extent practicable, to delete any personal data collected by the application that is stored by the developer; or (II) to refrain from any further use or sharing of such data; and (2) within a reasonable and appropriate time after receiving a request under paragraph (1)(B), comply with such request.[14]"

This provision incorporates within itself the right to be forgotten and makes it necessary for an application developer to either stop using or delete the stored data, within a reasonable time frame. Practically however, considering that the provision also can be brought into effect only when the user wishes to stop using the applicationand not before there may be very little a user can do till he/she continues to use the application.

Additionally, a major drawback is contained in Section 9, which provides that the Act, and its provisions shall apply 30 days after regulations made by the FTC under the Act, come into force[15] which means that, data collected and stored prior to such date shall not be protected. Another disappointing indication relating to the proposed legislation is that it has almost no chances of getting enacted into law, the website of the U.S. legislature shows that there is only a 1% chance of the Bill being passed.[16]

---

[14] Section 2 (b), Application Privacy, Protection, and Security Act of 2013 (draft)
[15] Section 9, Application Privacy, Protection, and Security Act of 2013 (draft)
[16] Govtrack.us, <https://www.govtrack.us/congress/bills/113/hr1913>

3. Children's Online Privacy Protection Act

Members of the House of Representatives introduced in 2011 a bipartisan legislation to amend the Children's Online Privacy Protection Act (COPPA)[17] and establish to other methods of protection for children. The proposed legislative amendment[18] prohibits the collection and use of minors' information for targeted marketing and would require service providers to allow the deletion of information of minors publicly available.

Data Protection & the European Union

"European data protection law first emerged within the framework of the Council of Europe. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was thus opened for signature by the member States of the Council of Europe in Strasbourg on 28 January 1981. Its purpose is to secure in the territory of each contracting Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him.[19]"

The European Union currently deals with data protection and privacy issues on the Internet vide the Data Protection Directive.[20] However considering that, "rapid technological developments have brought new challenges for the protection of personal data"[21] the European Union has felt the need for better protection mechanisms and consequently there is a proposal[22] to bring in a uniform single data

[17] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506
[18] Do Not Track Kids Act of 2011, H.R. 1895, 112th Congress (2011)
[19]Opinion of Advocate General Léger, delivered on 22 November 2005, European Parliament v Council of the European Union, Case C-317/04.
[20]Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[21] Committee Report, COM(2012) 11 final, [Proposal for a Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data].
[22] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, FTC Report.

protection legislation[23], which shall provide enhanced protection to the citizens of the member States. Though, the proposed European Union legislation aims to bring in sweeping changes to various areas of the law in the European Union, it has been heavily criticized by many who feel that it is full of many loopholes which will render it useless.[24]The areas of concern in the proposed European Union legislation include:

1. **Transparency**

The Explanatory memorandum to the proposed EU legislation provides for transparency and goes on to say that, "The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language is used. This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose. Given that children deserve specific protection, any information and communication, where processing is addressed specifically to a child, should be in such a clear and plain language that the child can easily understand.[25]"

This principle aims to put the onus on the data collector to have terms and conditions that are in simple and plain language, which are easy to understand. "As a general rule, any processing of personal data will require providing clear and simple information to concerned individuals as well as obtaining specific and explicit consent by such individuals for the processing of their data (Opt-in), other than in cases in which the data protection regime explicitly allows the processing of personal data.[26]"

<http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>

[23] Proposal for a Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

[24] Critics condemn new EU data-protection legislation, 22nd October 2013. <http://www.bbc.co.uk/news/technology-24622919>

[25] Explanatory Memorandum to the Proposal for a Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), paragraph 45.

[26]<http://www.mlawgroup.de/news/publications/detail.php?we_objectID=227>

The problem however will be the definition of the words 'clear and plain language' considering that there is no necessary definition of what is clear and plain in terms of language, additionally the word language has also been left undefined which would mean that the data collector shall be at liberty to use a language of his choice, considering the various member states of the European Union, this could end up being a situation where any language spoken a single member could be used. If one even assumes that the data collector shall use the language of the member state it operates from, considering the many languages in the European Union and the boundary free world the internet operates in, it would still not address the practical problem of a language the user in not aware of.

The other problem area will be the provisionrequiring that 'language a child user may understand' in cases where the user of the services would be a child. This requirement is on a plain reading difficult fulfill, considering that a child is a person below the age of eighteen.[27] It is important to note that, "the processing of data of individuals under the age of 13 will in general require parental consent, which will make it more difficult for companies to conduct business which is aiming at minors.[28]" However, even if one looks at the age group of children above the age of 13, who use the internet for learning and entertainment purposes, a requirement placing the onus on the provider to use language which is easy to comprehend for such a them child would be impractical. No matter what level of simple and clear language is used, very few children would understand the legal intricacies, in fact it is for these very reasons that contracts by minors are void under most jurisprudences. Additionally very few child users would ever even read lengthy privacy policies etc. and would simply accept them and proceed with using the application.

2. Consent

The consent requirements of the proposed EU legislation provide that, "Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that

[27]United Nations Convention on the Rights of the Child, Document A/RES/44/25(12 December 1989).
[28]<http://www.mlawgroup.de/news/publications/detail.php?we_objectID=227>

they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.[29]"

This provision would necessitate the data collector to have a mechanism, which would allow an individual to decide whether he/she wishes to consent to saving of private information. What is interesting is the provision requiring a positive act to denote consent instead of silence amounting to consent. However, it has also been argued that, "Consent does not deliver the level of protection that many think it does. Instead, it drives lazy, check-box compliance models—"he/she ticked the box, so now I can do whatever I like with their data." A modern law would acknowledge that, while consent will always be an important weapon in the privacy arsenal, it should not be the weapon of choice. There must always be other ways of legitimizing data processing and, perhaps, other than in the context of sensitive personal information, these should be prioritized over consent. At the same time, if consent is to play a lesser role in legitimizing processing at the outset, then the rights given to individuals to object to processing of their data once it has begun must be bolstered—without this, you place too much responsibility in the hands of controllers to decide when and why to process data with no ability for individuals to restrain unwanted intrusions into their privacy. There's a delicate balance to be struck, but a modern data privacy law would not shy away from finding this balance. Indeed, given the emergence of the Internet of Things, finding this balance is now more important than ever.[30]"

---

[29] Explanatory Memorandum to the Proposal for a Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), paragraph 25.

[30] Phil Lee, What a 21st Century Privacy Law Could – and Should – Achieve.<https://www.privacyassociation.org/privacy_perspectives/>

Another essential element is that the, "Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.[31]"

This provision is a great layer of protection offered to individuals, considering that very often employer's exercise a stronger position when dealing with employees and can often obtain consent which would not be given had the person concerned not been in the employer's employment.

Another interesting feature is the protection of personal data, which is related to fundamental rights or privacy. The proposal provides that, "Personal data which are, by their nature, particularly sensitive and vulnerable in relation to fundamental rights or privacy, deserve specific protection. Such data should not be processed, unless the data subject gives his explicit consent. However, derogations from this prohibition should be explicitly provided for in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.[32]"

Although, explicit consent is proof of the consent being informed, the legislation providing a protection in cases of 'legitimate interest' would be as a major loophole to the law. Jeremie Zimmermann from French consumer group *La Quadrature du Net* has expressed concern saying that, "A business could say that it is a legitimate interest

[31] Explanatory Memorandum to the Proposal for a Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), paragraph 34.

[32] Explanatory Memorandum to the Proposal for a Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), paragraph 41.

to collect data in order to provide a better service for consumers or to enable it to make money."[33]

For an application developer in particular, this argument would probably be available considering that most applications provided on mobile phones and on stores online are free but come with advertisements. The developer relies on revenue through advertisements in order to make his business viable and he may be able to argue that he has a legitimate interest in the information or also argue that the data collected can be used for advancements in the technology.

3. Privacy by Design

"The concept of 'Privacy by Design' is closely related to the concept of 'privacy enhancing technologies' or PET. This term was used for the first time in the report 'Privacy-enhancing technologies: the path to anonymity' that was published in 1995."[34] "Privacy by Design is an approach whereby privacy and data protection compliance is designed into systems holding information right from the start, rather than being bolted on afterwards or ignored, as has too often been the case.[35]" Peter Hustinx has expressed that, "the need for 'Privacy by Design' could never be better illustrated than by the increasing number of data security breaches that we have seen in recent years. As far as Europe is concerned, this is not only true for the UK, but also for other EU member states."[36]

What this essentially means is that the default setting of data collector's would be, to provide for privacy of data on their own instead of data deletion being requested for by the individuals. This although seems like a plausible option, it is difficult to implement considering many business models require data collection in order to survive. Most users would not opt-in to have their data collected and the consequent

---

[33] Critics condemn new EU data-protection legislation, 22nd October 2013 <http://www.bbc.co.uk/news/technology-24622919>

[34] Peter Hustinx, Privacy by design: delivering the promises. <http://link.springer.com/article/10.1007/s12394-010-0061-z>

[35] Information Commissioner's Office, U.K. <http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_by_design>

[36] Peter Hustinx, Privacy by design: delivering the promises <http://link.springer.com/article/10.1007/s12394-010-0061-z>

result would be that, most companies' whose primary source of income would be collection and dissemination of data to advertisers would need sweeping changes to business model's which would make their very survival possible.

In addition, considering that there is an exemption of public authorities exercising various functions to collect data, such a policy would seem discriminatory and may be labeled as an attempt at interfering with the right of an organization to trade and carry on business freely. It is often argued that, "engaging in free trade is a human right; it is not a battle that countries win or lose, it is an exercise of fundamental liberties for citizens to engage in voluntary transactions that leave participants better off.[37] The right to freedom of trade is not an absolute right, but one that governments should only circumscribe in the most adverse of circumstances."[38]

One may also bring up the right to freedom of expression as a ground to such a policy. As stated in *Autronic v. Switzerland*, the right to freedom of information "...applies not only to the content of information but also to the means of transmission or reception...any restriction imposed on the means necessarily interferes with the right to receive and impart information.[39]"

However, privacy by design is also voluntarily provided for by many applications. What is interesting is that many applications run two versions, a) a version which provides for advertisement free content but must be purchased paying money, and b) a version which may not have the same features or may be riddled with advertisements but can simply be downloaded for free. Privacy by design is a possibility in the web application market but it is certainly contingent on users paying for the application and its services.

4. Fair Information Processing

---

[37] Jeff Jacoby, *The Old Delusion of Protectionism*, Boston Globe January 10, 2010. <http://www.boston.com/bostonglobe/editorial_opinion/oped/articles/2010/01/10/the_old_delusion_of_protectionism/>

[38] Samuel Gregg, *Free Trade as Prosperity, Free Trade as Human Right,* August 25th, 2009. <http://www.thepublicdiscourse.com/2009/08/814/>

[39] (1990) 12 EHRR 485

"The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.[40]"

The principle of fair processing of information is certainly vital to proper data protection considering the fact that a data subject (user) may voluntarily grant consent for data collection to a particular entity for how it deals with the data, but would not be willing to grant that consent to other entities. Consent given to one data collector cannot mean that consent is given for the free sale of data in the open market. In addition, the right to be aware of how the information is processed and for what purposes it is collected is essential a feature for a user to give his/her informed consent.

An application developer can through his/her terms and conditions provide for details of why he is collecting the data, the recipient of such data, the use of this data and how the data subject can request for the deletion of the data. This obligation is least onerous and in fact would ensure that the data subject gives his consent as an informed user instead of blindly just agreeing.

5. The Right to be forgotten

"Any person should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the

[40] Explanatory Memorandum to the Proposal for a Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), paragraph 48.

processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation.[41]"

This feature of the proposed European Union legislation is akin to the one found in the U.S. Application Privacy, Protection, and Security Act of 2013, which requires that when a user withdraws consent to collection of data, he also has a right to have the data previously collected with consent to be deleted. Deletion of data that has no use for the data collector is definitely easier to comply with as compared with the other provisions of the law, arguably because the provision is applicable only to cases when the collector does not require the data for the purpose it was collected. The data collector can always use this provision to say that it still requires the data for purposes for which consent was granted and consequently this provision would not apply. The data collector would obviously not object to the deletion of the data it has no requirement for, considering that it would just be a waste of data space and nothing else if the data has no utility value.

A practical difficulty with this provision would be knowing the position of the data in fact, considering that the data subject would have no means to assess whether the data is still needed by the data collectoror whether the data collector has actually complied with the request for deletion. This provision would be based on complete trust on the working of the data collectors. Approach to the data protection authority would be a route that would be an unnecessary expense for both parties, something small application developers would be able to ill afford.

The explanatory memorandum of the proposal also goes on to say that, "This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health,

[41] Explanatory Memorandum to the Proposal for a Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), paragraph 53.

for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.[42]"

6. Practical Issues

There are certain key practical issues involved with the proposed European Union legislation:

(i) *Data Protection Officers in Each Member State*: critics of the legislation feel that the requirement for the creation of the post of data protection officers in all member States is quite cumbersome and an unnecessary requirement. Another criticism is that, users will have to approach the various data protection officers of the data collector's location to get redress.

(ii) *The Amount of fines:* The amounts sought to be imposed as fines are to the tune of up to EUR 100,000,000 or 5% of annual turnover[43] of a company globally. These amounts seem excessive and many start-ups would be unable to survive. The risk of violation would also be a dampener for any prospective developer from dealing with the European Union.

(iii) *Extra Territorial Applicability:* The law seems to cover not only the European Union and companies in its territory but also seeks to protect data of European Union citizens when it is dealt with outside the E.U.This provision would force many companies based outside the European Union to change business practices completely and adopt new models or to simply not deal with European Union citizens.

Conclusion

In conclusion, be it either the European General Data Protection Regulation or the plethora of proposed U.S. legislation, there is a changing trend towards data

[42] Explanatory Memorandum to the Proposal for a Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), paragraph 53.

[43] Eduardo Ustaran, EU Parliament Delivers - the World Awaits.
<http://privacylawblog.ffw.com/category/95-directive>

protection which requires developers to be careful when dealing with data. A web developer can certainly not ignore the inevitable policy and regulatory change of nations towards privacy. The ideal solution however would be to simply begin with self-regulation and reduce the dependence on data collection altogether. Companies pre-legislation should limit dependence on the sale or otherwise commercial dealing of user data as a source of revenue in order to avoid a situation where the company would have to hurriedly make drastic changes to its structure and functioning. An application developer can certainly not risk violating the regulations considering the high fines and can definitely safeguard its position best by always obtaining consent of the data subject, having an effective mechanism to deal with data privacy issues and most of all be commercially successful.