

Protecting Information Privacy on the Internet: Legal Framework in the EU

Dr Faye Fangfei Wang

Senior Lecturer in Law, Bournemouth University
89 Holdenhurst Road, Bournemouth BH8 8EB United Kingdom
Email: fangfei.wang@googlemail.com

Abstract

In the old ages, spies could enter one's residence, organizations or companies and collect valuable data information such as personal sensitive data, trade secrets or transaction records. Nowadays, the open architecture of the Internet has generated an environment in which it is much easier, quicker and wider to collect data than it used to be as a variety of sensitive information can be captured on the Internet without personal presence in the location where the data is situated. Privacy rights become more vulnerable to attack. This paper will discuss the current legal framework of ePrivacy protection in the European Union (EU), examine and evaluate practical obstacles and propose possible solutions to establish trust in private management.

1. Background of ePrivacy Protection

Privacy, as a fundamental human right, has been protected under basic laws in different countries or conventions at the international level since 1950s. From a boom of electronic commercial transactions in 2000, data protection stemming from International computer network has been challenged due to technical and legislative obstacles. Data protection constraints on the Internet are preventing them from fully protecting online users' privacy rights. In B2C transactions, an online retailer might have a database of information about its customers' personal details and their history of transactions. In B2B transactions, an international trading company might have its business partners' bank details and business strategies in their computer servers. So what will happen if a third party steals the information or if the database owner sells the information to the third party?

In order to build the web users' trust and confidence, online trading or service companies, have posted self-regulations on the webpage. However, it is doubted that how many users have actually read the privacy statement in small print or via a clicked link before using the service or placing the order. It is also suspected whether companies do keep their promises and comply with the self-regulated privacy policies. If not, what are the remedies?

In response to the necessity of e-privacy legislation, countries have made efforts to regulate the rules of e-privacy in order to facilitate economic growth, cooperation, trade and investment. This paper will discuss the current legal framework of ePrivacy protection in the European Union (EU), examine and evaluate practical obstacles and propose possible solution to establish trust in private management.

2. ePrivacy Legal Framework of the European Union

2.1 Current development

Data protection is to protect the rights of the data ownership and balance the benefits between the protection of the data ownership and the permission of data free-flow, whilst privacy protection is to protect fundamental human rights. In the EU, according to Article 1 of the EC Directive on Data Protection (1995), the EC Directive on Data Protection is not only to protect personal data but also individual privacy rights. The EC ePrivacy supplements the EC Directive on Data Protection. It reflects on Recital 6, 12 and Article 1 of the EC ePrivacy Directive. For example, Recital 6 of the EC ePrivacy Directive states that "the Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal *data* and *privacy*". Recital 12 further clarifies that it is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons". It also "harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community as stated in Article 1(1) of the EC ePrivacy Directive.

Although the EC ePrivacy Directive complements the EC Directive on Data Protection providing privacy protection particularly in the electronic communication sector, some provisions of the EC ePrivacy Directive are narrow or non-specific. For example, Article 4 Security and Article 6 Traffic Data need to be amended regulating the liability of data infringement. On 13 November 2007, the European Commission adopted a Proposal for amending the EC ePrivacy Directive. In response to the proposal, the European Data Protection Supervisor (EDPS) released his second Opinion on ePrivacy Directive review and security breach in January 2009. The EDPS welcomes the adoption of security breach notification system as it will encourage companies to improve data security and enhance the accountability of the personal data. That is, network operators and Internet Service Providers (“ISPs”) should notify security breaches to the National Regulatory Authorities (“NRAs”) and also their customers. However, it is argued that the communication is unclear in terms of its scope of the organization that is subject to breach notification as it seems to only refer to IT companies in the EU, whereas most state legislation in the US applies horizontally to all organizations that process certain types of information.

The substantial issue of the liability of infringement of privacy rights shall be governed by national laws. As stated in Recital 55 and Article 23 of the EC Directive on Data Protection, any person who has suffered damage is entitled to receive compensation from the controller, as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive. Article 15(2) of the EC ePrivacy Directive also provides that the provisions of judicial remedies, liability and sanctions of EC Directive on Data Protection shall apply with regard to national provisions adopted pursuant to this Directive. An example can be given by a leading case in the UK that hit the headlines in 2008. In the UK case of *Applause Store Productions Ltd and Firsht v Grant Raphael* (thereafter “Facebook” case [2008] EWHC 1781 (QB)), the claimant Mathew Firsht, the owner of Applause Store Productions, was successful in an action alleging libel and misuse of private information. It is a lawsuit against the claimant’s former friend, Grant Raphael, who created a false profile for Mathew Firsht on Facebook without his consent. The defendant published the claimant’s sensitive personal information on Facebook and created a link called “Has Mathew Firshts lied to you?” which defamed Mathew’s business in providing audiences for popular television program. The Judge Richard Parkes QC ruled that the claimant, Mathew Firsht was awarded £2,000 for damages compensation of his hurt feelings and distress caused by the defendant’s misuse of private information, along with the other compensation for damages of defamation. Thus, it is reasonably clear that damages in cases of misuse of private information are awarded to

compensate the claimant for the hurt feelings and distress caused by the misuse of their information.

From the discussion above, it is notable that the main privacy principles in the EC Directive on Data Protection are “notification”, “choice”, “security”, “data integrity” and “accessibility” and “accountability”. However, it does not include the principle of “enforceability”, which is recommended by the US Federal Trade Commission (FTC) in the EU- US Safe Harbour Agreement. Enforcement of privacy protection is one of the most complicated issues in information privacy protection. The legal certainty of enforcement of privacy protection is vital to build Internet users’ trust on web systems.

2.2 Future Solutions

In general, privacy policies are enforced either by national enforcement authorities, alternative dispute resolutions or court litigation. Those national enforcement authorities can impose sanctions or fine for privacy breaches. In the UK, the enforcement authority is information commissioner, whereas in the US, the enforcement authority is federal trade commissioner. Self-enforcement is also encouraged as both OECD “Privacy Online: Policy and Practice Guidance” in 2003 and FTC Fair Information Practices Report in 2000 found that fostering the adoption of self-regulatory enforcement mechanisms or initiatives, such as trustmark/seal programs, will be beneficial to promote effective global solutions with regard to privacy compliance. As stated in the FTC Fair Information Practices Report, “industry’s primary self-regulatory enforcement initiative has been the development of online privacy seal programs”.

A seal program, known as a “trustmark”, is usually accredited by a trusted third party and displayed on the authorised website. It is designed to build users’ trust on using the websites. It gives users certainty about the privacy policy standard on what kind of information a site gathers, what the site operator does with that information, and with whom that information is shared. The well-known seal/trustmark programs are TRUSTe, BBBOnline and VeriSign. Some companies’ websites have been licensed by the online privacy seal program. For example, eBay and Microsoft licensed by TRUSTe, Alibaba.com accredited by VeriSign etc. However, currently privacy seal programs were not widely supported by international and national legislation and only a relatively small percentage of sites introduced online-privacy seal program.

Both TRUSTe and BBBOnline have their enforcement procedures: users filing a complaint and seal program providers responding to a complaint by imposing sanctions on accredited websites. Such kind of sanctions may include:

- “1) requiring the Licensee to correct or modify personally identifiable information or change user preferences;

- 2) requiring the Licensee to change its privacy statement or privacy practices; and/or
- 3) requiring the Licensee to submit to a third-party audit of its practices to ensure the validity of its privacy statement and to ensure that it has implemented the corrective action required.”

However, seal program providers cannot require a Licensee to pay monetary damages or take further steps to exempt from legal violation. The compliant report will be published except for pre-agreement on confidentiality. TRUSTe and BBBOnline is the sole judge of the dispute.

Mann and Winn recognized such kind of complaint forum provided by TRUSTe and BBBOnline is an alternative dispute resolution (ADR) mechanism. In the author’s view, TRURSTe Watchdog Dispute Resolution Forum and BBBOnline Compliant Forum are not arbitration, mediation or negotiation as they are much lower than the standard of ADR procedures. It raises some concerns on why TRUSTe and BBBOnline do not offer normal online dispute resolution (ODR) procedures using a standard ODR platform, where a complainant can file a case and choose a neutral person such as an assisted negotiator, mediator or arbitrator to help resolving the case. TRUSTe and BBBOnline might save cost and avoid complication in the sole judgment, but it might be fairer, much more trustworthy or reliable and professional to adopt an efficient ODR procedure as cases of privacy breaches are usually not very simple. They require expert investigation.

Seal programs’ ODR service can be provided by any of the two means. The first method would be that seal program service providers could purchase or produce user-friendly ODR software and appoint qualified assisted negotiators, mediators and arbitrators. The second method would be that seal program service providers could form partnership with independent ODR service providers and publish the appointment agreement that seal accredited privacy-policy disputes would be resolved by their ODR partner. It is worthy of noticing that as mentioned earlier, eBay is accredited by the TRUSTe seal program, while eBay users’ disputes are compulsory to be resolved by SquareTrade (an ODR service provider) first before they go for litigation. In other words, eBay users have different channels to resolve different types of disputes, privacy-related issues on TRUSTe Watchdog Dispute Resolution Forum and business-related issues on SquareTrade. In these circumstances, it might make sense that SquareTrade is also designated to resolve eBay Users’ TRUSTe privacy-policy disputes to enhance the users’ confidence in providing personal information to proceed with commercial transactions.

3. Concluding Remarks

Trust and security are now, more than ever, critical issues in doing business, whether online or in the paper world. The development of global legislation in relation to data protection and information privacy becomes vital to facilitate international commerce.

One way to achieve legal certainty and predictability is through international harmonisation. Currently, the International, EU and US privacy legislation or guidelines have their different preferences. The EU legislation more aims at protecting individual privacy rights, whilst the US and International guidelines more targets at promoting the free flow of cross-border data for the development of global economy. There is one aspect in common, that is, they all make efforts on balance between individuals’ privacy rights and entrepreneurs’ marketing rights at the level of international harmonization. Trustmark program, provided by a trusted third party certifying the quality of merchants’ data privacy, should be deemed to be one of the most effective approaches in enhancing users’ trust and confidence in online interaction and transactions.

References

EDPS second Opinion on ePrivacy Directive review and security breach: privacy safeguards need to be strengthened, Press Release, Brussels, Monday 12 January 2009.

Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J. C 128/33, 6.6.2009.

Cooper, D., Fink, D., Jones, E., and Quathem, K. V. (2006), Security Breach Notification in Europe on the Horizon, World Data Protection Report, October 2006.

Privacy Online: Policy and Practice Guidance, OECD Working Party on Information Security and Privacy, DSTI/ICCP/REG(2002)3/FINAL, 21 January 2003.

Implementing the OECD ‘Privacy Guidelines’ in Electronic Environment: Focus on the Internet, Group of Experts on Information Security and Privacy, DSTI/ICCP/REG(97)6/FINAL, 09 September 1998.

Mann, R. J. & Win (2005), p.193. Electronic Commerce (New York: Aspen Publishing, 2nd Edition, 2005), p.227.