Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.15, No.1, 2024

The Right to Privacy of Customers of Financial Institutions vis-à-vis Credit Reference System: The Ethiopian Laws under Scrutiny

Misganu Degif Argne
School of Law, Wolkite University, PO Box 07, Wolkite, Ethiopia

Abstract
This study examined effects of credit reference system on the right to privacy of customers of financial institutions. The credit reference system being a medium for the exchange of personal information of customers of financial institutions taking part therein; aims at facilitating credit market efficiency and stability. The right to privacy on other hand tries to keep to the minimum the intrusion to private domain of persons, customers of financial institutions being one of them. This article critically examined how these two seemingly conflicting interests have been compromised under the Ethiopian laws. A doctrinal research approach was employed in the analysis of the Ethiopian laws on the right to privacy and laws governing the credit reference system**.** The review of literature and analysis of legal instruments of both national and international character have been used to substantiate the arguments set forth in this work.This work concluded that even though violation of the right to privacy of the customers of financial institutions can be justified on the ground of voluntary relinquishment such rights; the Ethiopian credit reference system still needs reconsideration in light of principles recognized internationally for the protection of the right to privacy of persons. This work recommends for the revision of the Ethiopian credit reference system for better protection of the right to privacy of customers of financial institutions.
Keywords: rights, privacy, credit reference system, financial institutions, Ethiopia
DOI: 10.7176/CEIS/15-1-03
Publication date: January 31st 2024

Introduction

The right to privacy in general and financial institutions' customer privacy protection in particular on the one hand and the credit reference system on the other has a competing role in the society. The right to privacy, as one of the internationally recognized human right, tries to keep to the minimum possible, the intrusion in to private life of individuals especially by placing a limit on the collection, processing, use and disclosure of their personal information by others (including individuals, private or public entities). On the other hand, the Credit Reference System serves as a medium whereby the credit information of borrowers could be shared among financial institutions authorized to use the system for the purpose of making a credit decision. Credit Reference System provides wide range of personal information of borrowers (information collected and submitted to the credit reference system by financial institutions) which could be accessed by many other financial institutions authorized to use the system to determine the creditworthiness of borrowers.

Despite its positive role for national economy in general and credit market efficiency and stability in particular, the credit reference system represents a threat to the privacy of individuals. In order to strike a balance between the rights to privacy on the one hand and sharing credit information in a Credit Reference System on the other, data protection principles have been incorporated in to the Credit Reference System. This article has tried to examine measures taken to protect customers' privacy in the Credit Reference System in light of personal data protection principles recognized under international data protection instruments. Particularly, Credit Reference System in Ethiopia under the governing National Bank directives has been scrutinized in terms measures taken to ensure the privacy of customers of financial institutions taking part in a Credit Reference System.

The article is organized in to three sections. The first section presents a brief account of the right to privacy under international human right and data protection instruments in general and the right to privacy under the FDRE Constitution and other subordinate legislations in Ethiopia in particular. The second section introduces the meaning, types, roles and privacy concerns of Credit Reference System in general and Credit Reference System in Ethiopia in particular. It also examines how privacy concerns on Credit Reference System are dealt with in light of the principles of personal data protection adopted under international data protection laws. The third section presents conclusions and recommendations.

Section One
The Right to Privacy
1.1. The Right to Privacy under Human Right Laws

The right to privacy is one of the internationally recognized human rights. Almost nearly all states' constitutions

and major international human rights instruments such as the Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR), European Convention on Human Right (ECHR), and American Convention on Human Rights (ACHR) have recognized the right to privacy of every one[1]. Common about the above mentioned human right instruments is that all of them have provided protection against arbitrary interference with privacy, family, home or correspondence and attacks upon honor and reputation of individuals.[2] Though the above mentioned human rights instruments have recognized the right to privacy, none of them have defined what is meant by privacy and the content thereof to which a legal protection is extended. They did not also clarify the sphere of life which can be considered private. It is only the case laws developed by the courts in the course of interpreting such instruments that have provided the detailed account of privacy. One of the institutions highly credited for developing a case law in this regard is the European Court of Human Right. The court, while ascertaining whether or not Article 8[3] of the European Convention on Human Right, has been violated on different occasions identified an illustrative list of acts which constitute violation of private life. Accordingly, based on the case law of the court , one of the matter an interference thereto fall under the scope of Article 8 (and further examined whether the interference was legitimate or not on the basis of sub-Article 2 of the same Article which provides for exceptions to the first sub-Article) is access to personal data.[4]

1.2. The Right to Privacy under Data Protection Laws

In the information age, the right to privacy has evolved to address issues relating to the collection, use, and dissemination of personal data in information systems. Further advancement in communication technologies have rendered insufficient the protection given to privacy and particularly to personal data under the human right instruments and it has led to the enactment of specific laws on protection of data both at national and international level. The notable legal instrument of international character adopted for the protection of personal data is the European General Data Protection Regulation (GDPR)[5]. The OECD Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data (here in after called OECD Privacy Guidelines)[6] and the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)[7] can also be mentioned as an important soft law instruments regarding the protection of personal data.

All of the above mentioned instruments have recognized that the right to the protection of personal data is one of the fundamental rights and freedoms of natural persons.[8]

All of the above mentioned data protection instruments have defined personal data in the same way as "*any information relating to an identified or identifiable natural person ('data subject')"*[9] Such a broad definition of personal data is said to have the potential to bring the majority of information within the scope of such data protection instruments.[10] Particularly the GDPR adopted the "identifiability" criterion which can be used in the ascertainment of the types of information through which a natural person may be identified. Accordingly, the GDPR states that "*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or*

** Lecturer of law, Wolkite University (LLB, LLM)

[1] See UDHR Article 12, ICCPR Article 17, ECHR Article 8 and ACHR Article 11

[2] Ibid.

[3] Article 8 titled *"Right to respect for private and family life"* states that 1) Everyone has the right to respect for his private and family life, his home and his correspondence.2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[4] In the case of (Rotaru v. Romania [GC], §§ 43-44, available at< https://hudoc.echr.coe.int/eng#{"itemid":["001-58586"]} , the court reached in to the conclusion that the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8, especially where such information concerns a person's distant past.

[5] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), OJ 2016 L 119/1. Available at < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> last accessed June 20, 2020.

[6] Organization for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Trans-border Flow of Personal Data,* 23 September 1980, available at: https://www.refworld.org/docid/3dde56854.html [last accessed 20 June 2020]. The privacy guidelines were first adopted in 1980 and revised in 2013 for the first time.

[7] The African Union Convention on Cyber Security and Personal Data Protection is adopted by the African Union in June 27, 2014 in Malabo, Equatorial Guinea. Available at< https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> [last accessed 20 June 2020] The Convention has not yet entered in force due to lack of the minimum number of ratification required for its entry in to force.

[8] See GDPR Article 1(2), *supra* note5 and the preamble of OECD Privacy Guidelines, *supra* note 6 and Malabo Convention, *supra* note 7.

[9] See Article 4(1) of GDPR and Article 1(b) of OECD Privacy Guidelines and Article 1 of Malabo Convention

[10] Andra Giurgiu and Thierry Lallemang, 'The General Data Protection Regulation: A New Opportunity and Challenge for the Banking Sector', 2017, P. 2. Available at
< https://www.researchgate.net/publication/313114747> last accessed June 18,2020.

social identity of that natural person."[1] It can, safely, be said that a broad range of personal data including a financial personal data are under the ambit of the above mentioned personal data protection instruments.

The OECD Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data has adopted eight principles (known as "fair information practices") governing the collection, use and disclosure of personal data and which have gained international acceptance[2] These are the principles of Collection limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation and Accountability.

The principles adopted by the OECD Privacy Guidelines has made an attempt to strike a proper balance between the rights to privacy particularly data subject's right to control personal data on the one hand and the free movement of information on the other hand. In order to protect the privacy right of data subjects, they are empowered to have control over the collection, use and dissemination their personal data. Accordingly, the data controllers are obliged to be compliant with rules and where appropriate to secure the consent of data subjects in the collection, maintenance, use and disclosure of such data.

On the other hand, in the interest of free movement of information, it is not always necessary to acquire the consent of the data subject for the collection, use and disclosure of such personal data. Such is the case where national sovereignty, national security and public policy ("*ordre public*") demands that personal data be collected, used and disclosed without the need to get the consent of the data subjects.[3] However, such exceptions are required to be as few as possible, and made known to the public.[4]

The GDPR have also adopted principles for the processing of personal data most of them are shared with those principles adopted under the OECD guidelines on privacy which every processor of personal data is obliged to comply with.[5] These are the principles of: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality and accountability. The Malabo Convention also adopted basic principles governing the processing of personal data which are more or less similar to those adopted under the OECD Privacy Guidelines.[6] These are the principles of: consent and legitimacy, lawfulness and fairness, accuracy, transparency, and confidentiality and security of personal data processing.

National constitutions also have been evolving to specifically recognize the control of personal data as a right and the governments of more than 60 countries around the world have adopted comprehensive data protection acts based on the fair information practices that apply to personal data held by the public and private institutions.[7] In the following section of this work the right to privacy and data protection is discussed under the Ethiopian laws.

1.3. The Right to Privacy under Ethiopian Laws

Ethiopia has recognized the right to privacy as one of the fundamental human rights under the supreme law of the land. Of course, this is in accordance with international commitments Ethiopia has subscribed to for the protection of human rights. In the same vein as those of major international human right instruments such as Universal Declaration of Human Right (UDHR) and International Covenant on Civil and Political Rights (ICCPR), the FDRE constitution has provided for the right to privacy without defining what privacy is.[8] The constitution rather listed what constitutes privacy. Accordingly, included under the right to privacy are the rights not to be subjected to searches of home, person or property, or the seizure of any property under personal possession of such persons. The constitution also provides for everyone's right to the inviolability of his/her notes and correspondence including postal letters, and communications made by means of telephone, telecommunications and electronic devices.[9] As such rights are not absolute; some limitation are made to such rights on account of safeguarding of national security or public peace, the prevention of crimes or the protection

[1] See GDPR Article 4(1), *supra* note 5.

[2] See Article 7-14 of OECD Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data. Of course such principles are also adopted under the national laws of some states such as U.S. Department of Health, Education and Welfare [1973]; and Canadian Standards Association International (CSA [1996]) and incorporated in to international treaties on data protection by the Council of Europe (1981) and the European Union (EC 1995); they have been also adopted by the UN General Assembly (1990) and the Commonwealth Secretariat (2002). See also David Banisar, *The Right to Information and Privacy: Balancing Rights and Managing Conflicts*, the World Bank; Access to information program, Working Paper, 2011 p.7.

[3] See Article 4 of OECD Privacy Guidelines, *supra* note 6

[4] Ibid.

[5] Article 5 of GDPR, *supra* note 5.

[6] See Article13 of Malabo Convention, *supra* note 6

[7] David Banisar, *The Right to Information and Privacy: Balancing Rights and Managing Conflicts*, the World Bank; Access to information program Working Paper, 2011 p.8. See also EPIC/PI (Electronic Privacy Information Center/Privacy International). 2007. *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments.* Washington, DC. < http://www.privacyinternational.org/survey/dpmap.jpg.> last accessed June 20,2020

[8] A Proclamation to Pronounce the Coming into Effect of The Constitution of The Federal Democratic Republic of Ethiopia, 1995, Proc. No.1, Federal Negarit Gazzeta, 1st Year No.1. Article 26.

[9] Id. Article 26(2)

of health, public morality or the rights and freedoms of others. However, such rights shall only be limited in compelling circumstances and in accordance with specific laws having the purpose of safeguarding national security or public peace, the prevention of crimes or the protection of health, public morality or the rights and freedoms of others.

The FDRE Constitution recognized the right to privacy in its rudimentary form as it doesn't cover many of the currently contending issues in the sphere of privacy especially in relation to the protection of personal data. Even though the constitution provided for protection against interference, except on the grounds stated thereunder, in to notes and correspondence including postal letters, and communications made by means of telephone, telecommunications and electronic devices, it does not say anything about the protection of personal data acquired and under the possession of public and private institutions in the course of discharging their responsibilities which have much relevance to the protection of privacy. In the information age, the right to privacy has evolved to address issues relating to the collection, use, and dissemination of personal data in information systems.[1]

As stated in above, while many states have recognized the right to control personal data under their constitutions, other states have enacted a comprehensive data protection laws that apply to personal data held by the public and private entities. Ethiopia has not yet enacted specific data protection laws. It should, however, be noted that there are scattered pieces of legislations which have relevance to the protection of personal data. Among such relevant legislations is Freedom of the Mass Media and Access to Information Proclamation[2].

Though the purpose of the Freedom of the Mass Media and Access to Information Proclamation, among other thing, is re-affirming right of media to collect and disseminate information, including information of a critical nature and the accessibility of information under the record of public bodies, it has some relevant provisions with respect to the protection of personal information under possession of public institutions. The proclamation has defined personal information as *"information about an identifiable individual"* and also provided illustrative lists of personal information. Among the lists of personal information under the proclamation are: information relating to the medical, educational or the academic, employment, professional or criminal history, of the individual or information relating to financial transactions in which the individual has been involved.[3]

The provision of the proclamation which has a direct relevance to this work is Article 17- which talks about how commercial information of third parties shall be disclosed by the public relation officer of the concerned public body[4]. Accordingly, the public relation officer shall refuse a

request for information if the requested information contains; a) trade secrets of a third party; b) financial, commercial, scientific or technical information, other than trade secrets, of a third party, the disclosure of which would likely to cause harm to the commercial or financial interests of that third party; or c) information supplied in confidence by a third party the disclosure of which could reasonably be expected to put that third party at disadvantage in contractual or other negotiations; or to prejudice that third party in commercial competition.

However, the public officer may not refuse a request for the accessibility of the record in so far as it consists of information: already publicly available; or in relation to which a third party did not object to the disclosure[5] or has consented in writing to its disclosure to the requester concerned. Public bodies in possession of the records of personal information are duty bound to maintain the confidentiality of such information and they can disclose such information only on grounds recognized under the law. One of the grounds upon which a public body may disclose such personal information of a third party to the requester of the information is the consent of the individual to whom the information relates.

Consent might be given before or after the submission of the information to the public bodies. The public bodies may inform individuals before the submission of the information that the information belongs to a class of information that would or might be made available to the public. Accordingly, if the individual to whom the information relates agree that his/her personal information to be made available to the public, the public bodies can disclose such information to the requester without notification and seeking further consent of the individual concerned. On the other hand, consent for the disclosure of personal information under the possession of the public bodies to a requester might be given after the submission of such information to the public bodies. This

[1] David Banisar, '*The Right to Information and Privacy: Balancing Rights and Managing Conflicts'*, the World Bank; Access to Information Program Working Paper, 2011 p.6. Available at < https://www.ip-rs.si/fileadmin/user_upload/Pdf/Publikacije_ostalih_pooblascencev/Right_to_Information_and_Privacy__banisar.pdf> last accessed June 21, 2020.

[2] A Proclamation to Provide For Freedom of the Mass Media and Access to Information, 2008, Proc. No.590, Federal Negarit Gazzeta, 14th Year No.64

[3] Id. Article 2(8)

[4] Public body is defined under the proclamation as "anybody established under the Federal Constitution or state constitution or any other law which forms part of any level or branch of the federal or regional state or owned, controlled or directly or indirectly substantially financed by funds provided by the federal or regional governments or accountable to the federal or regional states." id. Article 2(5).

[5] Id. Article 19

happens when the individual to whom the information, the disclosure of which sought, relates to has not given his/her consent upon the submission of such information. Accordingly, the public officer of the concerned public body, when he intends to disclose confidential personal information submitted by third party, has to notify his/her intention of disclosing personal confidential information under the possession of the public body to that third party who has supplied the information.[1] And this enables the third party either to protest or consent to the proposed disclosure. Failure to protest within 15 days from date of issuance of the notice gives rise to the presumption that he/she has consented to the disclosure.

As it can be inferred from the above mentioned provisions of the proclamation, an effort is made to strike a balance between protections of the right to privacy on the one hand and the accessibility of information under the record of public bodies on the other. In the following part of this work, credit information system as a mechanism for the protection of privacy and ensuring the accessibility of financial information among financial institutions is discussed.

Section Two

2. Credit Reference System and Privacy Concerns under the Credit Reference System

In this section, credit reference system in general and how it works in Ethiopia with due regard to the protection of customer privacy on the one hand and sharing of personal information of the customer within the circle of financial institutions in particular is discussed.

2.1. The Meaning and Role of Credit Reference System in General

Credit reference is one of the methods used by lenders for the assessment of the credit worthiness of their potential borrowers. Credit reference provides detailed information on person's on credit history, including information on their identity, credit accounts and loans, bankruptcies and late payments, frauds and forgeries, cheque kiting, false declarations, receiverships, bankruptcies and liquidations, credit default and late payments, false securities use and misapplication of borrowed funds.[2] Such information on credit history of persons (individuals or institutions) is provided by credit reference (credit reporting) institutions. Credit reference institutions can be owned either publicly or privately.[3] While Credit Bureaus (CB) are privately owned credit reference institutions, Public Credit Registries (PCR) is publicly owned credit reference institutions.[4] PCR is usually operated by the central bank or a financial supervisory authority and it could be regarded as a form of government intervention, taking charge of the compulsory function of information sharing in the credit market[5]. On the other hand, Credit Bureau as a privately owned entity which pursues profit and tends to cater to the information requirements of commercial lenders.[6]

The major difference between a CB and a PCR is in the nature of information sharing. While a CB voluntarily shares information among members, a PCR is a legal requirement.[7] The other difference noted between the two is that while data collected by CB are often more comprehensive and better geared to assess and monitor the creditworthiness of individual clients, PCR are often geared towards collecting system-wide information for macro-prudential and other policy purposes.[8]

Credit reference institutions, be it Credit Bureau or Public Credit Registry, play a significant role on financial institutions' decision on whether or not to grant a loan to potential borrowers by providing information (including personal information) about borrowers. In many countries, lenders routinely share information on the creditworthiness of their borrowers. This happens through the instrumentality of Credit Bureau or Public Credit Registry. Private credit bureaus receive data about borrowers from the respective lenders and they collate this information with data from other sources (courts, public registers, tax authorities, etc.) and compile a file on each borrower.[9] Lenders can obtain a return flow of consolidated data about a credit applicant by requesting a "credit report" from the bureau.[10] Credit reports issued by credit bureau range from simple statements of past defaults or

[1] Ibid.
[2] MOSES KARONG'A NG'ANG'A, 'The Effect Of Credit Reference Bureaus Information Sharing on Non-Performing Loans In Commercial Banks', 2015, (International Journal of Business and Commerce Vol. 5, No.03), P.3.available at < https://www.ijbcnet.com/5-3/IJBC-15-5211.pdf> last accessed June 22,2020
[3] World Bank(2016),Credit Bureau: Definition And Comparison To Credit Registries, available at <https://www.worldbank.org/en/publication/gfdr/gfdr-2016/background/credit-bureau > last accessed June 20,2020
[4] Ibid.
[5] Kwangsuk Han et al**, '**Legal Frameworks and Credit Information Systems in China, Korea, and Singapore',2013 (Asian-Pacific Economic Literature, The Australian National University and Wiley Publishing Asia Pty Ltd.) p.147-148, available at https://onlinelibrary.wiley.com/doi/pdf/10.1111/apel.12007 last accessed June 20,2020
[6] Ibid.
[7] Ibid.
[8] World Bank (2016), *supra* note 27
[9] Tulli Jappelli and Marco Pagano, 'Role and Effects of Credit Information Sharing',(2005), Center for Studies in Economics and Finance (CSEF) WORKING PAPER NO. 136 available at https://core.ac.uk/download/pdf/6925878.pdf> last accessed June 17,2020
[10] Ibid.

arrears − "negative" data – to detailed reports on the applicant's assets and liabilities, guarantees, debt maturity structure, pattern of repayments, employment and family history − "positive" data.[1]
On the other hand, Public Credit Registry are generally managed by central banks, and access is granted only to authorized central bank staff (mainly for surveillance reasons and under tight confidentiality rules) and to the reporting financial institutions.[2] Accordingly, this creates a two-way flow of data between credit grantors and the Public Credit Registry, as in the case of private credit bureaus.

Transparent credit information is a prerequisite for sound risk management and financial stability.[3] Generally, the literature has identified four effects of information sharing by credit reference institutions on credit market efficiency and stability. These are[4] 1) improving banks' knowledge of applicants' characteristics, easing adverse selection problems; 2) reducing the "informational rents" that banks could otherwise extract from their customers; 3) act as a borrower disciplining device, by cutting insolvent debtors off from credit; and 4) eliminating or reducing the borrowers' incentive to become "over-indebted" by drawing credit simultaneously from many banks without any of them realizing.

2.2. Privacy Concerns in Credit Reference System

Despite its positive role for national economy in general and credit market efficiency and stability in particular, the credit reference system represents a threat to the privacy of individuals. Sharing credit information of borrowers among lenders or financial institutions in a credit reference system has a far reaching implication on privacy of such borrowers or customers of the lenders or financial institutions. As stated above, the information collected and shared within the credit reference system includes personal information (both positive and negative information) of customers of lending institutions taking part in a credit reference system. Sharing information within a credit reference system does not only disclose the personal information of individuals, but also harms their future opportunity of accessing credit in almost all financial institutions especially where such information are about customers history of default in payment of debt.

Accordingly, an apparent contradiction is observed between laws governing credit information sharing on the one hand and laws designed to protect the right to privacy on the other. Different countries have treated such contradictions in their own ways and the way it has been treated said to have had profound effects on the development of credit information systems.[5] Some countries strict privacy protection laws goes so far that it had prevented the development of private credit bureaus in those countries[6]. Tulli Jappelli and Marco Pagano have categorized countries, in terms of the level of protection given to privacy against credit information sharing, in to three groups[7]. These are 1) Low-protection countries, such as Argentina, where anyone can access all debtors' data regardless of the purpose of investigation; 2) Medium-protection countries as the United States, data can be accessed only for an "admissible purpose", essentially the granting of credit; and 3) Higher level protection countries, such as France and other European countries, where borrower's explicit consent is required in order to access his/her personal file.

In the final analysis, the suggested solution would be the adoption of a balanced approach which could maintain the benefits of credit reference system to the national economy in general and to the credit market efficiency and stability in particular while assuring customers' privacy protection in the system. In order to strike a proper balance between protection of customers' privacy on the one hand and the promotion of credit reference system in the interest of national economy on the other, some principles, which imposes a limitation on personal data collection, use, processing and disclosure by both private and public entities, have been adopted both at the national and international level. As discussed in the previous sections of this work, the principles adopted under some international legal instruments such as OECD Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data and the European General Data Protection Regulation (GDPR) and incorporated in to the domestic laws of states for the protection of personal data are applicable to personal data in the credit reference system as well. The principles are: collection limitation, purpose specification, openness, security safeguard, data quality, use limitation, individual participation and accountability.

Against this backdrop, in the following section of this work credit reference system and the treatment of privacy under the relevant national bank directives in Ethiopia is discussed.

---

[1] Ibid.
[2] Ibid.
3 World Bank(2016),Credit Bureau: *Definition And Comparison To Credit Registries*, available at <https://www.worldbank.org/en/publication/gfdr/gfdr-2016/background/credit-bureau >
[4] Tulli Jappelli and Marco Pagano, *supra* note 33,p.9, see also MOSES KARONG'A NG'ANG'A , *supra* note 26, p.11
[5] Tulli Jappelli and Marco Pagano *supra* note 33, p.24
[6] Ibid.
[7] Ibid.

2.3. Credit Reference System and Customer Privacy Protection in Ethiopia

2.3.1. Credit Reference System in Ethiopia

The National Bank of Ethiopia (NBE) is empowered under the new Banking Business Proclamation, which repealed and replaced the previous Licensing and Supervision of Banking

Business Proclamation No. 84/1994, to issue a directive for the establishment, operation and cost apportionment of a credit information sharing system among banks.[1] The credit information sharing system established by Directive No SBB 36/2004 under the repealed banking business proclamation was repealed and replaced by Credit Information Sharing Directive No CRB/01/2012 under the current Banking Business Proclamation and again the later one was replaced by a new directives called the 'Establishment and Operation of Credit Reference Bureau Directives No. CRB/02/2019' (herein after called the Credit Reference Directives). Accordingly, the following discussion is based on this later directive which is currently applicable to the credit reference system in Ethiopia.

As stated earlier, credit reference institutions are categorized, based on their ownership structure, in to private and public credit reference institutions. The Ethiopian credit reference system is of the latter type and is established and operated by the National Bank of Ethiopia (NBE) through its Credit Bureau which is one of its operational work unit.[2]. Financial institutions licensed by the National Bank of Ethiopia such as banks, micro-finance institution and capital goods finance company, from the effective date of the directives, are not allowed to extend new or renew or reschedule or refinance existing loans unless they are registered with the Credit Reference System.[3] Accordingly, it is mandatory for such financial institutions in Ethiopia to participate in the Credit Reference System.

The Directive defined Credit Reference System as *"computerized credit reference data base system set up by the National Bank to facilitate the function of Credit Reference Bureau in which provision, updating and correction of credit information rendered by financial institutions and enquiries of credit information on borrowers and other related activities of financial institutions are carried out electronically through a dedicated computer system or network."*[4]

On the basis of the definition, the four basic tasks to be accomplished under the credit reference system are: 1) Provision of credit information by participating financial institutions to that of the Credit Reference System; 2) Updating credit information already supplied by the financial institutions to the Credit Reference System; 3) Correction of error files submitted by financial institutions to the Credit Reference System; and 4) Enquiries of credit information on borrowers.

Credit information is defined as "all information about a borrower and the borrower's credit account(s) as specified in the Data Standardization Manual and/or Data Submission Specification."[5] On the other hand, Data Standardization Manual and/or Data Submission Specification is a manual which is part of the Directive and provides the standard data reporting requirement on borrowers, loan account(s), collateral, guarantor, stakeholders and other similar credit information.[6] Financial institutions are required, as one of the regulatory requirements, to submit credit information about their borrowers to the Credit Reference System, which will be stored in the Credit Reference System and will be accessed by all participating financial institution, based on the Data Standardization Manual and/or Data Submission Specification prescribed by the National Bank of Ethiopia. The Credit Reference Bureau does not directly collect credit information from borrowers for it is not a lending institution rather such credit information are collected and submitted to the credit reference system by participating financial institutions on the behalf of the Credit Reference Bureau. A wide variety of personal information including negative information about borrowers or borrowers' credit account(s) is required to be submitted to the Credit Reference System.

2.3.2. Credit Reference System and Customer Privacy Protection in Ethiopia

The credit information about borrowers submitted by one of the participating institutions can be accessed, for the purpose of making credit decision, by all the other participant of the Credit Reference System. Accordingly, personal information of the customer (borrower) of one of such institutions would be revealed, through the credit reference system, to all other institutions taking part in the credit reference system whenever they have to make credit decisions on loan application in which the customers have been involved either as a borrower or guarantor. This has, definitely, posed a threat to the privacy of customers of financial institutions taking part in the credit reference system. In the remaining part of this section, the Ethiopian credit reference system is examined the extent to which it has provided customers' privacy protection in light of the principles for the protection of privacy under international legal instruments discussed in the preceding sections of this work.

[1] A Proclamation to Provide for Banking Business, Proc. No. 592, 2008, Federal Negarit Gazetta, 14th year No.57. Article 57
[2] 'Establishment and Operation of Credit Reference Bureau Directives, Article 4(1)
[3] Id. Article 5(1) and Article 8
[4] Id. Article 2(7)
[5] Id. Article 2(4)
[6] Id. Article 2(8)

The principles are collection limitation, purpose specification, openness, security safeguard, data quality, use limitation, individual participation and accountability

1. Collection Limitation Principle

Regarding the manner of collection of personal data, the principles dictate that such data should be collected in a lawful manner and where appropriate with the knowledge or consent of the data subject.[1] Under the Credit Reference Directives, credit information about a borrower or his/her guarantor is, supposedly, to be collected where the financial institutions received a loan application from potential borrowers.[2] The person making a loan application to financial institutions is presumed to know that his/her personal information, which are necessary to make the decision by that institutions on whether or not to grant a loan to the applicant, will be collected and processed by the such financial institution. Furthermore, financial institutions have a legal obligation to collect and evaluate the relevant personal information of a loan applicant in order to decide on such loan applications. On the face of such legitimate grounds, the collection of personal information of borrowers by the participating financial institutions of the credit reference system is in accordance with principles for the protection of privacy.

2. Data Quality Principle

Once personal data has been collected through a lawful means, the next issue, with respect to protection of privacy, is ensuring the quality of such information; otherwise it could misrepresent the data subjects. For this reason, the personal data collected by data controllers is required to be accurate, complete and kept up-to-date.[3] The Credit Reference Directives imposes an obligation on participating financial institutions to submit to the Credit Reference System credit information which is correct, accurate, complete and timely updated.[4] Furthermore, financial institutions are duty bound to update the credit information about their borrowers which they have been initially submitted to the credit reference system on an ongoing basis. While banks are required to update such credit information once in a month, microfinance institutions and capital good finance companies have a duty to update such information once in a quarter.[5] Since participating financial institutions have initially a duty to submit to the Credit Reference System credit information which is correct, accurate, complete and timely updated, they are made responsible for any damages, claims or liabilities that may arise as a result of inaccurate, misleading or incomplete credit information on borrowers supplied to the credit reference system by individual financial institutions and shared through it with other financial institutions.[6]

3. Purpose Specification Principle

The other point which has a far reaching implication on the protection of privacy in the process of collection and use of personal information is the specification of purposes for which such information is to be collected. Since the data subject consents for the collection of their personal data on the understanding that such data will be used for a specific purposes by the data collectors/controllers, any subsequent change of purpose by the data collectors alone is against the will of the data subjects. The purpose for which such data are to be used should be specified not later than at the time of data collection and the subsequent uses should be limited to the fulfillment of those purposes.[7]

The Credit Reference Directives requires that each participating financial institutions to receive from their borrowers and guarantors written and signed off consent for the sharing of borrower's or guarantor's credit information among all other financial institutions and to access their credit information maintained with the Credit Reference System.[8] Since participating financial institutions have a duty, as one of the regulatory requirements, to submit credit information on their borrowers to the Credit Reference System, it can be said that one of the purposes of collecting such credit information from their borrowers is to submit it to the Credit Reference System. Even though, the ultimate purpose of collecting credit information is to make a decision on credit application, sharing such information to other financial institutions could be another purpose. Accordingly, borrowers of financial institutions, while giving their consent for the sharing of their information with other financial institutions, have the possibility of knowing that for what purpose their personal information is to be used.

4. Use Limitation Principle

Personal data should be used only for purposes originally specified at the time of the collection of such data and for purposes the data subjects have consented for. Personal data can, therefore, be used for purposes other than for which it was originally meant for only with the consent of the data subject or where the law authorizes.[9] As stated above, participating financial institutions are required to receive a written and signed off consent of their

[1] OECD Privacy Guidelines, *supra* note 6, paragraph 7
[2] Credit Reference Directives; *supra* note 43, Article 7(1)
[3] OECD Privacy Guidelines, *supra* note 6, paragraph 8
[4] Credit Reference Directives; *supra* note 43, Article 7(2, 7).
[5] Id. Article 7(4)
[6] Id. Article 6(2)
[7] OECD Privacy Guidelines, *supra* note 6, paragraph 9
[8] Credit Reference Bureau Directives; *supra* note 43, Article 7(1).
[9] OECD Privacy Guidelines, *supra* note 6 paragraph 10

borrowers and guarantors for the sharing of borrower's or guarantor's credit information among all other financial institutions and to access their credit information maintained with the Credit Reference System. The Credit Reference Directives strictly forbids the use of credit information on borrowers obtained from the Credit Reference System for purpose other than making a lending decision or during activities pertaining to account management procedures or periodic portfolios reviews conducted by financial institution on its borrower.[1] Participating financial institutions are not even allowed to query the credit reference system unless there is a genuine credit application submitted to such institutions by borrowers or for purposes of account management procedures or periodic portfolio reviews.[2]

Credit information obtained from Credit Reference System should be treated with the utmost confidentiality and the institutions are permitted neither to disclose such information to third party nor to use for any other purposes. The Credit Reference Bureau has also an obligation to maintain the Credit Reference System in a secured manner and with strict confidentiality.[3]

5. Security Safeguards Principle

Protecting the privacy of data subjects entail putting in place a security safeguard to the protection of such personal data against the risk of loss or unauthorized access, destruction, use, modification or disclosure of data.[4] In this regard the Credit Reference Directives imposes an obligation on the Credit Reference Bureau to ensure access to the Credit Reference System is given only to authorized persons.[5] On the other hand, participating financial institutions are required, in order to ensure the integrity and security of data, to make sure that the Credit Reference System at the financial institutions is operating with strict data access procedures.[6]

Accordingly, it can be said that the Credit Reference Directives, which governs how Credit Reference System is to be used, has put in place mechanisms for safeguarding the security of personal information of borrowers in a Credit Reference System and this has a paramount importance for the protection of the privacy of customers of the financial institutions.

6. Openness Principle

Openness of the system maintaining personal information to the data subjects regarding its operation helps to build a trust on the system and thereby ensure the protection of privacy by the system. Accordingly, data controllers should have general policy of openness about developments practices and policies with respect to personal data and means should be available to establish the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.[7] As far as the general openness of the Credit Reference System with regard to its policies and practices about credit information to the borrowers is concerned, the Credit Reference Directives has no explicit provisions except that it has provided for how borrowers can access their credit information in the credit reference system, which will be discussed under the next theme.

7. Individual Participation Principle

It is only where the data subjects have an access to their personal information under the possession of the data controller that they can challenge its reliability and, if the challenge is successful, their data can be erased, rectified, completed or amended. Accordingly, individuals should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them and to have communicated to them, data relating to them within a reasonable time, in a reasonable manner and in a form that is readily intelligible to them.[8]

The Credit Reference Directives provided for how borrowers or guarantors of a participating financial institution can access their credit information in the Credit Reference System. Borrowers or guarantors can access their credit information in the Credit Reference System in three occasions.[9] First, if they are in dispute about their own credit status with their lending financial institution, they may obtain their credit information from the Credit Reference System upon payment of fee to be set up by the National Bank. Second, they may obtain their credit information from the Credit Reference System free of charge at the time when financial institutions start processing their applications for additional new loan, restructuring or renewal of the existing loan. Thirdly, they may obtain their credit information from the Credit Reference System free of charge once in a period of 12 consecutive months. Borrowers' and guarantors' access to their credit information gives them a chance to challenge the reliability of such information under the Credit Reference System which could be shared among all participating financial institutions in making credit decisions with respect to such borrowers or

[1] Credit Reference Bureau Directives; *supra* note 43, Article 7(12, 14).
[2] Id. Article 7(14)
[3] Id. Article 6(2)
[4] OECD Privacy Guidelines, *supra* note 6 paragraph 11
[5] Credit Reference Bureau Directives; *supra* note 43, Article 6(4).
[6] Id. Article 7(11)
[7] OECD Privacy Guidelines, *supra* note 6, paragraph 12
[8] Id. Paragraph 13
[9] Credit Reference Bureau Directives; *supra* note 43,, Article 4(4), 7(15).

guarantors.

The Directives have also provided for how complaints may be lodged by borrowers regarding the accuracy of their credit information to the participating financial institutions and, if not satisfied with the decision of such institutions, to the Credit Reference Bureau and the time framework within which both the participating financial institutions and the Credit Reference Bureau shall responds to the complaint[1].

Since customers (borrowers) have an access to and the right to challenge the accuracy of their credit information in the Credit Reference System and the right to have them corrected, if their complaint is found to be legitimate, individuals participation in the Credit Reference System enhances the protection of privacy of customers of the participating financial institutions.

8. Accountability Principle

In order to ensure data subject's right to privacy, data controllers should be made accountable for complying with measures which give effect to the principles.[2] The Credit Reference Directives have provided for penalties of various types starting from written warning and financial penalties to the suspension of financial institutions from using the Credit Reference System based on the repeated nature of violation of the provisions of the Directives by such institutions.[3] The Directives particularly punishes violation of the provisions dealing with the submission of correct and updated credit information, the regular updating of such information and correction of error files. The accountability of participating financial institutions for submission to the Credit Reference System of inaccurate or misleading credit information on borrowers could be taken as a good move to the protection of privacy of customers (borrowers) of such financial institutions.

Section Three
Conclusion and Recommendations
3.1. Conclusions

The right to privacy in general and financial institutions' customer privacy protection in particular and the credit reference system (through which credit information of borrowers of financial institutions could be shared among many other financial institutions) seems to contradict each other. As stated earlier in this work, the right to privacy is one of the internationally recognized human rights and it gives protection to individuals against arbitrary interference with privacy, family, home or correspondence and attacks upon honor and reputation. This has been recognized under the major international human right instruments and FDRE constitution as well.

In a more specific level, the right to privacy tries to keep at best to the minimum possible, the intrusion in to private life of individuals especially by placing a limit on the collection, processing, use and disclosure of their personal information by others (including individuals, private or public entities). This is so because, in this age of information, it is neither possible nor desirable to ban totally an access to personal information of individuals by others. Consequently, the right to privacy in the context of personal information is understood to be individuals' right to control the collection, processing, use and disclosure of their personal information by others. This has been recognized by data protection laws both at national and international levels.

On the other hand, the Credit Reference System serves as a medium whereby the credit information of borrowers could be accessed by financial institutions to make a credit decision. Credit Reference System provides detailed information on person's on credit history, including information on their identity, credit accounts and loans, bankruptcies and late payments, frauds and forgeries, false declarations, receiverships, bankruptcies and liquidations, credit default and late payments, false securities use and misapplication of borrowed funds. Credit Reference System provides a lot of personal information which could be used by financial institutions authorized to use the system to determine the creditworthiness of borrowers. Transparent credit information is a prerequisite for sound risk management and financial stability and this could be met through Credit Reference System. Despite its positive role for national economy in general and credit market efficiency and stability in particular, the credit reference system represents a threat to the privacy of individuals. This so because the Credit Reference System serves as an instrument for the sharing/disclosure of personal information about borrowers to many financial institutions thereby puts the privacy of borrowers at risk.

In an attempt to strike a balance between the two competing interest i.e. privacy protection and accessibility of information, data protection laws both at national and international level have introduced principles designed to protect the privacy of individuals while ensuring the free flow of information. The two prominent data protection laws of international character are the OECD Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data and the European General Data Protection Regulation (GDPR). Principles adopted under such legal instruments and incorporated in to many domestic data protection laws includes the principle of collection limitation, purpose specification, openness, security safeguard, data quality, use limitation, individual participation and accountability. The principles are applicable to all types of personal information

[1] Id. Article 9
[2] OECD Privacy Guidelines, *supra* note 6 paragraph 14
[3] Credit Reference Bureau Directives; *supra* note 43, Article 11.

(including credit information) under the possession of both public and private institutions.

Though Ethiopia is not a party to any international data protection laws and has not yet enacted a comprehensive data protection laws, most of the principles of data protection have been recognized under some its domestic legislations such as Freedom of Media and Access to Information Proclamation and most importantly under the laws governing Credit Reference System. The governing laws on credit reference system in Ethiopia are the National Bank of Ethiopia's Directives on Establishment and Operation of Credit Reference Bureau: Directives No. CRB/02/2019. As discussed in above, the Directives have tried to keep a balance between the protection of customers (borrowers or guarantors) privacy on the one hand and the sharing of credit information about borrowers or guarantors among financial institutions taking part in a Credit Reference System on the other.

The Directives have provided mechanisms for the protection of the privacy of customers of financial institutions taking part in the Credit Reference System. The requirement of written and signed off consent of borrowers for the collection and sharing of their credit information to other financial institutions through Credit Reference System; financial institutions' obligation: to use such information only for the purpose of making credit decisions, to safeguard the security and integrity of such information, to ensure the quality and accuracy of their borrowers' credit information and not to disclose such information any other third party; borrowers right to access and challenge the accuracy of their credit information in the Credit Reference System; and the accountability of financial institutions for violation of the provisions of the Directives are among the measures taken by the Credit Reference Directives to protect the privacy of customers(borrowers or guarantors) under the Credit Reference System. Accordingly, it can, safely, be said that the Directives have embraced most of the principles adopted under international data protection laws designed protect privacy of data subjects.

However, there are still some issues which need be addressed especially in relation to how and when financial institutions should respond to borrowers' request to access their credit information. Even though the Directives have provided for borrowers' right to access to their credit information in the credit reference system, it does not provide for how (responding electronically or in written form) and in what period of time should financial institutions respond to borrowers' request for access to their credit information.

3.2. Recommendations

As discussed in the above, the Credit Reference Directives has not provided for how and when should the participating financial institutions respond to borrowers' request for access to their credit information. Since how and when customers' of the participating financial institutions can have an to access to their credit information in the credit reference system plays a significant role on the protection of privacy, it is recommend that the future revisions of the Directives to regulate: 1) how (electronically or in written form) financial institutions should respond to borrowers' request for access to their credit information in the credit reference system; and 2) the time frame within which participating financial institutions should respond to borrowers' request for access to their credit information in Credit Reference System in the future revisions of the Directives.

List of References

Legislations

1. 'Establishment and Operation of Credit Reference Bureau Directives No. CRB/02/2019'
2. A Proclamation to Pronounce the Coming into Effect of The Constitution of The Federal Democratic Republic of Ethiopia, 1995, Proc. No.1, Federal Negarit Gazzeta, 1st Year No.1
3. A Proclamation to Provide for Banking Business, Proc. No. 592, 2008, Federal Negarit Gazetta, 14th year No.57. Article 57
4. A Proclamation to Provide For Freedom of the Mass Media and Access to Information, 2008, Proc. No.590, Federal Negarit Gazzeta, 14th Year No.64

International Legal Instruments

1. Organization for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Trans-border Flow of Personal Data,* 23 September 1980, available at: <https://www.refworld.org/docid/3dde56854.html>
2. Organization of American States (OAS), American Convention on Human Rights, "Pact of San Jose", Costa Rica, 22 November 1969, available at:< https://www.refworld.org/docid/3ae6b36510.html>
3. Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, available at: https://www.refworld.org/docid/3ae6b3b04.html
4. EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), OJ 2016 L 119/1. Available at < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
5. *The United Nations. Universal Declaration of Human Rights*. 1948. Available at < https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf>
6. UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at: https://www.refworld.org/docid/3ae6b3aa0.html

Journal Articles

1. Andra Giurgiu and Thierry Lallemang, 'The General Data Protection Regulation: A New Opportunity and Challenge for the Banking Sector, 2017 Available at < https://www.researchgate.net/publication/313114747>
2. David Banisar, 'The Right to Information and Privacy: Balancing Rights and Managing Conflicts', the World Bank; Access to information program Working Paper, 2011 p.6. Available at < https://www.ip-rs.si/fileadmin/user_upload/Pdf/Publikacije_ostalih_pooblascencev/Right_to_Information_and_Privacy__banisar.pdf>
3. Kwangsuk Han et al**, 'Legal** Frameworks And Credit Information Systems in China, Korea, and Singapore',2013 (Asian-Pacific Economic Literature, The Australian National University and Wiley Publishing Asia Pty Ltd.) p.147-148, available at <https://onlinelibrary.wiley.com/doi/pdf/10.1111/apel.12007>
4. MOSES KARONG'A NG'ANG'A, 'The Effect Of Credit Reference Bureaus Information Sharing on Non-Performing Loans In Commercial Banks', 2015, International Journal of Business and Commerce Vol. 5, No.03, P.3.available at < https://www.ijbcnet.com/5-3/IJBC-15-5211.pdf>
5. Privacy and Human Rights 2006*: An International Survey of Privacy Laws and Developments.* Washington, DC. < http://www.privacyinternational.org/survey/dpmap.jpg.>
6. Tulli Jappelli and Marco Pagano, 'Role and Effects of Credit Information Sharing', 2005, Center for Studies in Economics and Finance (CSEF) WORKING PAPER NO. 136 available at <https://core.ac.uk/download/pdf/6925878.pdf>
7. World Bank(2016),'Credit Bureau: Definition And Comparison To Credit Registries', available at <https://www.worldbank.org/en/publication/gfdr/gfdr-2016/background/credit-bureau >