Summer 5-27-2016

Network externalities in biometrical identification

Reima Suomi
Turku School of Economics, University of Turku, Finland

Network externalities in biometrical identification

Reima Suomi[1]
[1]Turku School of Economics, University of Turku, Finland

Abstract: Biometrical identification has not been adopted to be a key technology in computer security as was hoped for, or to the extent the sophistication of the technology would promise. One reason for this might be that the application of biometrical identification has not yet gained wide enough scale, which leads to missing positive network externalities.In this paper the concepts of biometrical identification and network externalities are discussed, and an analysis is performed on why missing positive network externalities are hampering the advance of biometrical identification.

Keywords: Biometrical identification, network externalities, computer security

1. INTRODUCTION

Biometrical identification has not grown up to its potential [1], [2], [3]. The technology itself of course has shortcomings, but even more there are shortcomings in the understanding of economic aspects and functioning of the biometrical identification market. One important aspect of that are network externalities. The user and developer community of biometrical identification can be seen as a network, where network externalities materialize themselves. As the community grows larger in size, and the connections between the nodes of the network strengthen themselves, network externalities are to establish themselves. If biometrical identification is expected to prosper and proceed, the network should take active steps to minimize negative network externalities, and to strengthen positive network externalities. This task is not made easy by the vague and by definition hidden nature of network externalities. This article adopts a network and network economics point of view to biometrical identification.

The article unfolds as follows. First, a short wrap-up of what is biotechnology is provided. Second, network externalities are defined and used. If one takes a look at these two sections, biotechnology analysis is for reference purposes only, but the discussion on network externalities is providing more new perspectives and frameworks, as overreaching and summarizing material on this topic is scarce.

Finally, the major contribution of this paper is the marriage of these issues. Problems with biometrical identification technology dissemination are discussed from the network externalities point of view. It is concluded that the biotechnology market is too small and young to provide positive market externalities and to fight against negative network externalities. A conclusion to follow is that economics analysis must be performed more on biometrical identification technology, starting from basic economics concepts, such as network externalities discussed in this paper.

This paper is conceptual in nature, and contains no direct empirical work.

2. BIOMETRICAL IDENTIFICATION

The need to identify persons accurately is a key need of any – especially modern – society. Biometrical identification that has actually been the cornerstone of identification ever (people are known traditionally because of their race, age, size and face characteristics). Another popular method has been that of handwriting, where the connection between the person and the signature is always anyway vague.

These traditional kinds of identification have been very natural, but they cannot happen over the telecommunication network. The new network economy where identification must happen without being

simultaneously at the same place necessitates new kinds of identification practices. Special devices, methods and applications are needed for biometrical identification over the networks[4].

Authentication methods are found inthree categories: what you know (for example usually password and/or PIN), what you have (for examplesmart card), and what you are (for example biometric technologies) [5]. The category of "what you are", also biometric identification, is of course the easiest and most user-friendly option for the end-user, as no active action from his/her side is needed, just "being what you are" is enough.

Biometric authentication is based on the measurement of a physical or behavioral trait that makes each individual unique. It compares a person's unique characteristics, such as the fingerprints, face, or retinal image, against a stored set profile of these characteristics to determine whether there are any differences between these characteristics and the stored profile. [6]

Biometric control devices use special-purpose sensors to measure and digitize a biometric profile of an individual's fingerprints, voice, or other physical trait. The digitized signal is processed and compared to a previously processed profile of the individual stored on magnetic disk. If the profiles match, the individual is allowed entry into a computer network and given access to secure system resources. [7]

The key difference of biometrics to other digital identifiers, such as passwords, PINs or credit cards is that biometrics cannot be lost or forgotten; since biometric measurements are part of the body, they will always be present when needed. [8]

Most usual biometric techniques are (adapted from [7]):

- Dynamic signature verification
- Face geometry
- Finger scan
- Hand geometry
- Passive iris scan
- Retinal scan
- Voice print.

New technologies that are difficult to counterfeit do emerge. A big trend is that of using many different biometrical identification methods simultaneously, adopting to the current identification situation[9]. Vein pattern technology or blood vessel authentication is considered being a secure technology, with the benefit that blood vessels do not change or wear with age. Moreover identification does not require touching any device as the patterns are captured with a high resolution infrared camera. Other new applications of possible growing importance or that are being developed are based on traits such as 3D ear recognition, lips, odor, gait and keyboard strokes [10, 23-24]. Relying on traits such as gait or keyboard strokes, is neither relying on what you *know*, what you *have* nor on who (or what) you *are* but on what you *do*.

3. NETWORK EXTERNALITIES

Networks externalities, both positive and negative, are known to be part of every network[11]. Positive network externalities are the main reason for building networks, and a primary source of wealth for the modern society, often actually called the network society [12, 13, 14]. Network externalities stemming from telecommunication networks are a primary source of wealth in the information society. Taking this seriously, it is astonishing how little effort information system researchers have devoted to understanding network externalities.One reason might be that network externalities have traditionally been a playfield of economists, and information system researchers have felt unease at the field.This, however, needs not to be the case.Aside the rather theoretical discussion on network externalities the economists run, a more practical and operative approach to the issue is needed.

According to a recent research, network externalities are one of the 10 key forces that drive information technology to the society [15]. For economists, the theory of network externalities, or network externalities, or standardization, has wide applicability.Indeed, it has fundamental importance for competition policy, regulation, business strategy, intellectual property, and technical change in a wide range of industries; developments in these industries cannot be fully understood without an understanding of network externalities [16].

Network externality has been defined as a change in the benefit, or surplus, that an agent derives from a good when the number of other agents consuming the same kind of good changes [17].

Network externalities are a popular and important theoretical concept, yet very much neglected by the information systems research community.Because of this, there remains a risk that their operationalization of network externalities in the field of information networks is not conducted properly.

The roots of the network externality research are in the marketing discipline, where it was understood that the success of a product or service is a phenomenon strengthening itself. The phenomenon was called the bandwagon effect by which was meant *"the extent to which the demand for a commodity is increased due to the fact that others are also consuming the same commodity. It represents the desire of people to purchase a commodity in order to get into 'the swim of things'; in order to conform with the people they wish to be associated with; in order to be fashionable or stylish; or, in order to appear to be 'one of the boys.*"[18]

Network externalities can be direct or indirect.Direct network externalities exist when an increase in the size of a network increases the number of others with whom one can "communicate" directly. Indirect network externalities exist when an increase in the size of a network expands the range of complementary products available to the members of the network [16].

Network externalities can be positive or negative.A typical negative network effect is a traffic jam.All too often network externalities are understood just as positive.The same phenomenon can be both positive and negative, depending on the role of the observer.To take an example, to a railway operator having a lot of customers is a good thing (more revenue), but for the customer the same situation can mean congestion, also a negative effect. The enchantment of network externalities is that they often come out as surprise and as a byproduct that was not calculated or foreseen in any way.

Using biometrical identification happens in a social and market interaction, also in a network. In Figure 1 we have summed up main potential network externalities in the application of biometrical identification as identified by the author.It must be remembered that network externalities by definition materialize in an unexpected way, and so any such list must always be seen as tentative and as a kind of "best guess".

Type of effect \ *Causality*	*Direct*	*Indirect*
Positive	• Decreasing device, system andtechnology prices as the market grows • Possibility for positive user testimonials and experiences	• Increased awareness of body condition for citizen • New business opportunities for biometrical identification product and service providers • New user interface expectations of users
Negative	• Increased hygienic risks • Fear on losing of privacy	• Less business for prochicers of traditional lock and other access control device manufactures • Less transparent procedures for users • New challenges for ICT education

Figure 1.Network externalities in biometrical identification

Below we discuss each item in Figure 1 in detail.As in almost any market, even in the biometrical identification market the price of products and services is to decrease as the market grows, because of scale advantages.Unfortunately, this process is first taking its initial steps, and biometrical identification at least has a reputation of being an expensive technology, which often too is also true.

A key factor for any technology is user acceptance [19], [20], [21], [22], [23]. Positive user experiences documented in customer testimonials, and word-or-mouth marketing, often in new social media, are crucial to the success of a new technology.Unfortunately, still we have very little documentation on positive user experiences of biometrical identification.

The world has become very sensitive to contact-disseminated diseases such as SARS or Swine influenza (also called pig influenza, swine flu, hog flu and pig flu).This was not the case in the pioneering days of biometrical identification.Nowadays, any biometrical identification that is based on physical contact is doomed to have difficulties in this aspect.The risk of contamination of course grows as the number or users, the network, grows bigger.

Biometrical data if any is very sensitive. Humans fear very much loss of sensitive data. The bigger the data bases and user communities of biometrical identification, the bigger the risk value of a possible privacy violation.

Biometrical identification means the exposure of your body for some kind of scanning.This means increased awareness for humans of their body condition. This kind of increased awareness might lead to positive health effects, as people more eagerly begin to take care of their body.In the opinion of the author, this might be the biggest and most positive network externality of biometrical identification ever.

Innovators and forerunners in biometrical identification are going to have competitive advantages, as long as their service offerings are successful.Biometrical identification might become a key industry for many countries, serving the whole economies with positive growth effect. In practice, however, biometrical identification is so integrated with other, more traditional information technology, that newcomers might have difficulties in entering the market. Traditional ICT service and equipment providers clearly have a competitive advantage.

Biometrical identification user interfaces must be very flexible and of high quality. This might have a positive impact on the whole user interface development of the ICT sector.User interface, again, is known to be a key component in the productivity of computer work. One might expect that advances in biometrical identification user interfaces might give a boom to the whole productivity of computerized work.

Introducing new technology is always an innovation process, where older innovations have to give way[24, 25]. In computers, the changes to software might not be so revolutionary, actually more changes are to be seen in the new needed hardware components.On the contrary, in the locking and entrance controls of physical facilities, biometrical identification solutions might substitute classical solutions, such as traditional locks based on physical keys. This means losing of business for those producers.

Biometrical identification is a complex set of theory, technologies, equipment, architectures, standards and applications.Average computer user is sure to lose oversight of the technology.Worse still, security and privacy technology is something that is purposefully kept secret. However, this means low transparency of the systems, and further low user acceptance. Traditional security solutions are often more easy to understand.

The need for new knowledge on biometrical identification is huge.Research and education on the issue must be intensified. This of course is also a positive challenge, but must be seen also as a burden for the research and education community. A lot of society resources must be devoted to research and education activities on biometrical identification

4. CONCLUSIONS

Biometrical identification threats to remain an eternal promise that never materializes to a mature technology [26]. Traditionally, reasons for its success or non-success has been sought from its technical characteristics of biometrical identification[27].

This article took a different point of view to the issue.From the theory of network externalities popular in economics, reasons for the good and bad function of the biotechnology product and services market were sought. Unfortunately, a lot of reasons were found why positive network externalities are not materializing in this market, and why negative network externalities prevail.

In general, the whole market of biometrical identification is still too small. Products and solutions cannot be produces in big enough scale, and prices remain high. Positive user experiences are scarce, and so user pressure to introduce new technology is low. Learning curve of the users and producers – the whole industry – is still flat, and on the other hand the technology is far from perfect – maturation of the technology is also low.

The market is also dominated by classical players in the ICT-industry. We might see the same situation as in the car manufacturing.The much better and wanted technology of electric cars is not proceeding, as their development is conducted by traditional car makers, who have a lot of benefits to watch in the old technology.

One more promising avenue for advancing biometrical identification might come from medicine and related sciences. Hygienic and contamination risks of biometrical identification – especially in the case of physical contact with jointly used devices – should be taken seriously. A huge positive network externality might come from the increased attention of people to their body.Awareness of body condition in general will most certainly lead to better care-taking of the body.This population health effect is more than worth thriving for.

In general, biotechnology must be seen from other perspectives than technology.Maybe we should talk about bio-solutions for identification. Medical, market and economic aspects of these solutions must be studied in more depth.

REFERENCES

[1] Ruoti, S., Roberts, B., and Seamons, K. (2015) Authentication melee: A usability analysis of seven web authentication systems, In Proceedings of the 24th International Conference on World Wide Web, pp 916-926, International World Wide Web Conferences Steering Committee.

[2] Rankin, D. M., Scotney, B. W., Morrow, P. J., and Pierscionek, B. K. (2012) Iris recognition failure over time: The effects of texture, Pattern Recognition 45, 145-150.

[3] Gong, S., Cristani, M., Yan, S., and Loy, C. C. (2014) Person re-identification, Vol. 1, Springer.

[4] Zhang, D. D. (2012) Biometric solutions: For authentication in an e-world, Vol. 697, Springer Science & Business Media.

[5] Kroenke, D. M. (2007) Using MIS, Pearson Education. Prentice-Hall, Upper Saddle River, New Jersey.

[6] Laudon, K. C., and Laudon, J. P. (2006) Essentials of business information systems, Pearson Education. Prentice-Hall, Upper Saddle River, New Jersey.

[7] O'Brien, J. A., and Marakas, G. M. (2006) Management Information Systems, Seventh International Edition ed., McGraw-Hill, New York.

[8] De Hert, P. (2005) Biometrics: legal issues and implications, European Commission, Brussels.

[9] Rattani, A. (2015) Introduction to Adaptive Biometric Systems, In Adaptive Biometric Systems, pp 1-8, Springer.

[10] European Biometrics Portal. (2006) Biometrics in Europe-Trend Report June 2006.

[11] Morasch, K. (2015) Cooperation and competition in markets with network externalities or learning curves, Springer.

[12] Castells, M. (1996) The rise of the network society, Blackwell Publishers Inc., Malden, Massachusetts.

[13] Stalder, F. (1998) The rise of the network society, the information age: Economy, society and culture, vol I, Information Society 14, 301-308.

[14] Brandsen, T., Trommel, W., and Verschuere, B. (2015) The state and the reconstruction of civil society, International Review of Administrative Sciences, 0020852315592467.

[15] Andal-Ancion, A. (2003) The digital transformation of traditional business, MIT Sloan Management Review, 35-41.

[16] Besen, S. M. (1999) Innovation, Competition, and the Theory of Network Externalities, Charles River Associates.

[17] Liebowitz, J., and Margolis, S. E. (1998) Network externalities (Effects), In The New Palgrave's Dictionary of Economics and the Law.

[18] Leibenstein, H. (1950) Bandwagon, Snob, and Veblen Effects in the Theory of Consumers' Demand, The Quarterly Journal of Economics 64, 183-207.

[19] Shih, H.-P. (2004) An empirical study on predicting user acceptance of e-shopping on the Web, Information & Management 41, 351-368.

[20] Hsu, M.-H., and Chiu, C.-M. (2004) Internet self-efficacy and electronic service acceptance, Decision Support Systems 38, 369-381.

[21] Wang, Y.-S., Wang, Y.-M., Lin, H.-H., and Tang, T.-I. (2003) Determinants of user acceptance of Internet banking: an empirical study, International Journal of Service Industry Management 14, 501-519.

[22] Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003) User acceptance of information technology: Toward a unified view, MIS Quarterly 27, 425-478.

[23] Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S., and Reich, C. (2015) A Survey of Continuous and Transparent Multibiometric Authentication Systems, In Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015, p 1, Academic Conferences Limited.

[24] Dhanaraj, C., and Parkhe, A. (2006) Orchestrating innovation networks, Academy of Management Review 31, 659-674.

[25] Christensen, C. M. (2013) Disruptive innovation, *The Encyclopedia of Human-Computer Interaction, 2nd Ed.*

[26] Loughlin C. Keeping an Eye on Biometrics. Sensor Review. 2006; 26: 4.

[27] Cavoukia A, Stoianov A. Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy. Ontario: Information and privacy commissioner/Ontario, 2007.