TO TRADE OR NOT TO TRADE? THOUGHTS ON THE FAILED SMART CARD BASED NATIONAL ID INITIATIVE IN TAIWAN

Tyng–Ruey Chuang[1] Jan–Ming Ho[1] Shih–Kuen Huang[1]

Ching–Yi Liu[2] Da–Wei Wang[1]

Abstract

While the emergence of the digital economy is undoubtedly creating exciting opportunities for Asian countries and it is a popular prediction that smart cards would be the next technological transition, the upheaval associated with them is producing profound changes and challenges. Attracted either by business reasons or mass dataveillance efficiency, some Asian countries, including South Korea and Taiwan, have initiated governmental projects to implement full scale smart card based national ID schemes for the past several years. For the present these governmental projects have either been delayed or canceled.

Based upon an account as to how the smart card based national ID system projects in Taiwan and South Korea failed to succeed under strong protests, this paper elaborates why the scheme seems to become a particularly favored strategy for some Asian governments, especially those who already have national ID card systems in place for several decades, to adopt in vitalizing or escalating their electronic commerce. It is followed by an analysis on how this kind of projects could be examined through the lens of achieving long-term success of digital economy and preserving online privacy. We conclude that before we have a sensible argument about the future technological and legal architecture of electronic commerce, public values such as privacy protection should be preserved, as they contribute to electronic commerce significantly in the long run.

[1]Drs. Tyng–Ruey Chuang, Shih–Kuen Huang, and Da–Wei Wang are assistant research fellows, and Dr. Jan–Ming Ho, a research fellow, at Institute of Information Science, Academia Sinica, Nankang, Taipei City 115, Taiwan. Their e-mail addresses are {trc, skhuang, wdw, hoho}@iis.sinica.edu.tw.

[2]Ching–Yi Liu, J.S.D., is an assistant professor of law at Tamkang University, Tamsui, Taipei County 251, Taiwan. Her e-mail address is tgcn143@ibm.net.

1. Introduction

While the emergence of the digital economy is undoubtedly creating exciting opportunities for Asian countries [30] and it is a popular prediction that smart cards would be the next technological transition [6, 12], the upheaval associated with them is producing profound changes and challenges. Attracted either by business reasons or mass dataveillance efficiency, some Asian countries, including South Korea and Taiwan, have initiated governmental projects to implement full scale smart card based national ID schemes for the past several years. For the present these governmental projects have either been delayed or canceled. In the case of South Korea's proposed electronic national ID card project, the result of presidential election in December 1997 and the economic crisis forced South Korean government to reconsider the project [23]. As the Taiwanese case has shown us, a public request for proposals was announced in June 1998 by the authority, the IC Card Planning and Promotion Task Force [31]. It follows that four proposals had been submitted and a consortium was selected in August to negotiate a contract with the government. It turned out the deal broke down and no contract was signed in late November 1998 amid strong public protests from non-governmental organizations. However, it was reported that the government has been considering a second round initiation to save the project for smart card based national ID system.

Based upon an account as to how the smart card based national ID system projects in Taiwan and South Korea failed to succeed under strong protests, this paper elaborates why the scheme seems to become a particularly favored strategy for some Asian governments, especially those who already have national ID card systems in place for several decades, to adopt in vitalizing or escalating their electronic commerce. It is followed by an analysis on how this kind of projects could be examined through the lens of achieving long-term success of digital economy and preserving online privacy.

2. Smart Cards and National ID Systems in Asia

There is no denying that the power of smart cards should never be understated in the digital age [6]. While credit and debit cards have a magnetic stripe containing limited information about the cardholder, a smart card, a credit-card size plastic card with an

embedded central processing unit (CPU) and random access memory (RAM), is equipped with all the memory and processing functions its name implies. Once a smart card is inserted into a reader, it could be activated to exchange data with the reader, and to exchange data with a remote server connected to the card reader via network. Under this smart card architecture, it seems very easy to track and record the use of a particular card. As a result, it is conceivable that electronic ID systems supported by smart card technologies would be haunted by controversies about possible violations of personal privacy.

As a matter of fact, the necessity and appropriateness of creating a national ID scheme has long been a controversial issue in countries around the world. In United States, the proliferation of the social security number (SSN) for purposes unrelated to the administration of the social security system, and the use of SSN to uncover or link databases on many aspects of a person's life, have disturbed many civil libertarians [16]. In addition, whether it is appropriate to utilize SSN as the individual identifier for the health ID card system [26], as well as whether all Americans should receive a health identifier under the health care system, gave rise to privacy and security concerns [32]. Similarly, proposals for a national ID system had been confronted by oppositions both in Australia and New Zealand. The Supreme Court of Philippine struck down an administrative order authorizing the adoption of its national computerized identification reference system in the summer of 1998 [9].

On the other hand, however, for countries who already have a national ID card system, to further computerize their systems proves to be an irresistible temptation. In Singapore, for example, not only the universal resident ID has a bar code, its government employee and military personnel have used smart card based ID cards for years. The fascination with "digitalized nation" has prove to be equally irresistible for South Korea and Taiwan, as they each has planned to adopt a smart card based national ID system.

Several East Asian countries, such as Japan, South Korea, and Taiwan, long have the practices of maintaining a "resident administration system" by a government agency to keep track of their people's movement and household information. In Taiwan, for example, the law requires timely report to the government agency about changes of the

family's addresses and members. Under this context, the resident administration system has the potential to serve as the foundation of a surveillance society. In Taiwan, again, the local resident administration office is where a citizen applies for his/her national ID card. Also mandated by the law, a person is supposed to carry with him/her the national ID for purposes of conducting various daily transactions both in the public and private sectors. For instance, the national ID is widely used as a person tries to apply for a job, to see a doctor with his/her health insurance plan, to get a credit card or passport, to cash a check, to cast his/her vote, and so on. It seems beyond all imagination for a citizen to lead a life without a national ID in Taiwan. Although resident administration system is closely related to the national ID card, some countries, such as Japan, has never implemented any national ID scheme even though it does have a resident administration system.

As mentioned briefly earlier, the year of 1998 witnessed several ambitious efforts to implement full scale smart card based national ID schemes in at least three Asian countries: South Korea, Malaysia, and Taiwan. South Korean government has pushed for one of the world's most extensive national ID card projects since mid-1990s. This project, Electronic National Identification Card Project, was given birth by the cooperation of the Ministry of Domestic Affairs and the Korean Computer Institute. Under this project, a smart card would be used to integrate various ID cards, including current universal ID card, resident registration card, driver's license, national pension card, medical insurance certificate, and scanned fingerprints, among others [23]. After 50 billion won (Korean dollars) has been invested on building the preliminary infrastructures, the plan was stalled in early 1998 primarily due to South Korea's national economic hardship and finally canceled in 1999 [4, 5]. It is also worthwhile to mention that civil rights groups in South Korea have been strongly opposed to the project, and the project became an issue during South Korea's 1997 presidential election.

A similar project was set in motion in Malaysia originally aimed at giving every resident of the city of Kuala Lumpur a smart card. It seems that Malaysian government has planed to make it a flagship application of its full-scale Multimedia Super Corridor project [27]. The Malaysian project covered more than the South Korean one did. The national ID card, which might be accompanied by a secondary card, would support financial purposes such as those performed by an e-cash card, ATM card, or debit card. It

was reported that the project had been delayed, probably also due to Malaysia's recent financial difficulties.

3. A Chronicle of the Taiwanese Initiative

The Taiwanese initiative to implement a smart card based national ID system might be the most complicated one known today, especially the way it would be financed. As mentioned earlier, the national ID system in Taiwan has been in existence for decades, and has become an almost inseparable part of one's everyday social transactions. Every ten years a new ID card, which might takes a new format, is issued to every citizen.

Accidentally, in 1995, a national health insurance scheme was introduced in Taiwan. The compulsory scheme covers every citizen (except those in military service). Insured person is issued a health insurance certificate that carries, among others, the name and date-of-birth of the bearer, as well as his/her national ID number. The certificate does not carry a photo; hence, it must be used with the patient's national ID card to prevent abuse of medical resources (e.g., sharing a certificate among several people). There are six cells at the back of the certificate and, for every visit to a doctor, a stamp with the name of the medical provider as well as the date of the visit is placed in a cell. After six visit, the used certificate must be returned to the Bureau of National Health Insurance (NHI) in exchange for a new one. This is viewed as a mechanism to control cost as people who visit doctors often will turn in their certificates as often. For those chronically ill or with major health problems, a separated certificate is issued and its usage is exempted from the six-visit restriction. Starting in 1996, a pilot project has been conducted in Penghu county (a group of islands separated form the main Taiwan island) to use a smart card based certificate. The motivation seems to be cost control: The frequency of medical visits can be recorded on the chip in the patient's certificate, and uploaded to the NHI server if necessary. Another major difference is that the smart card based certificate also carries the bearer's photo while the old one does not. Hence, the new health insure certificate also becomes a general-purpose ID card in many situations.

Subsequently, at the recommendation of the Steering Committee for Information Development and Promotion, a cabinet-level ad hoc committee, an "IC Card Planning

and Promotion Task Force" was formed in July 1997 to look into the feasibility of using a smart card to combine the functions of the national ID card and the health insurance certificate. The task force is under the guidance of the Research, Development and Evaluation Commission (RDEC), a cabinet-level body, but includes representatives from various governmental departments (MOI and NHI among them), university professors, and business interests. It is not clear why the later two groups of people are included in the task force. The task force then moved quickly in the direction of producing a plan in which the government would not have to pay for the cost of implementing the smart card based national ID system. The cost is to be borne by some private sector company in exchange for exclusive rights of using the system for e-commerce purposes, which by one estimation is a 600 million US$ business for a 10-year period.

On June 10, 1998, a final request for proposals was announced, culminating previous announcements starting from April that year [31]. At that time, the general public was not aware of the government's plan, though one of us (C.─Y. Liu) had started monitoring the event and wrote op-ed articles on major newspapers [24]. To seize the business opportunities, four private sector consortiums were formed in a very short period of time to compete for the government contract. Consequently, four proposals were submitted and one of them was selected by a committee in August to negotiate a final contract with the government. At this point, the public started to notice the plan, perhaps because of several op-ed articles written by us [20], and the continued argument between the civil rights groups and the government that followed [29]. Legislation hearings were held, as were several workshops where the issues were openly debated. By November 25, the negotiation between the government and the selected consortium broke down, citing fundamental disagreements over card-issuing fees, as well as value-added business opportunities allowed within the proposed system [3].

Despite it has been claimed that advanced computer security technologies would be utilized in the proposed project in Taiwan to avoid the misuse and abuse of personal information, the project has received harsh public criticism for potential violation of privacy since mid-1998. Some civil libertarians and academic groups have relentlessly raised security and privacy concerns on the one-card-does-all "citizen card" scenario, which has been described by government authorities as the most efficient way to create a

wired country [31].

Furthermore, just as the question of individual consent, that is, under what kind of legal and technical architecture would an information subject not only have a say over how his or her information is used, but also have the right to withdraw it completely if they wish, is a tricky one. Civil libertarians in Taiwan and South Korea have questioned whether the ultimate truth about the proposed smart card based national ID card schemes is they are bringing us a Big Brother era of electronic surveillance [11, 18].

Nevertheless, it was also reported recently (May 1999) that the government is now considering to fund the project on its own, so that it could be implemented as soon as possible, and the operation might be transferred to the private sector later on. It is not clear yet whether the revitalized project would survive public scrutiny.

4. Online Privacy under the Emergent Smart Card Based National ID Regime

The Taiwanese plan, as detailed by the the government's Request for Proposal (RFP), is to issue a "Citizen's Card" that will incorporate the functions of various identification cards (with the national ID and the health insurance certificate being two of them), and to provide the necessary electronic signature and identification mechanisms needed for secure e-commerce and on-line identification [31]. It will also be a test case of the government's so-called "total outsourcing policy" for contracting out the operations of governmental information systems. It aims to create an environment to stimulate the growth of relevant industries as well.

Although it was unclear from RFP what financial service functions would be available under the proposed plan at the outset, it seems obviously that a potential contractor could add electronic purses and debit card functions in the future. According to a leaked document from the selected consortium, a fully-fledged e-commerce framework is planned upon the proposed ID system. Note that, in particular, the RFP indicates that memory space in the card may be used for the development of electronic commerce, and "while maintaining the principle of protection of personal information, the card shall provide fields for basic personal data and an electronic signature mechanism that may be

freely read by interested parties" [31]. According to the RFP, the citizen card would include sensible personal data such as the number of times and the places a person receives medical treatment, and whether those are special medical treatment. It also includes two digitalized thumb-prints and a digitalized photo, in addition to various personal data (name, date-of-birth, national ID number, and so on).

We were brought to a new landscape that is more variegated and hopeful than before, it seems few efforts have been made to consider the issue of online privacy in a global sense — how digital technologies would affect the very nature of privacy and whether regional and cultural factors would come into play in the discourse on the technological transformation of privacy. One of the primary dangers stemming from the smart card based national ID card system is the mass dataveillance made possible by the comprehensive database of integrated personal information of the whole population. From the perspective of privacy protection, it is unacceptable to have a national central databank supported by the smart card based national ID card system. It is true that smart card technology is one of the most secure devices in the digital age [15], however, it is also undeniable that techniques now unknown may be used to break into what we consider secure now [7, 8]. In addition, a smart card itself might be only one component of security in a system, the possibility of breaches in other system areas could not be excluded. Moreover, non-technological factors, such as social, economical, and cultural ones, which vary significantly from society to society might determine how secure a smart card system would be to a great degree.

Given the complexity to predict the possible subsequent uses and processing on personal information both by the public and private sector, it seems citizens in Taiwan and South Korea would be forced to live under the smart card based national ID regime without being fully informed of the influences the schemes might have on them (and possibly their descendants). Furthermore, as there are only very loose and out-of-dated personal information privacy protection laws in Taiwan and South Korea, it is also widely questioned how the consenting rights of information subjects would be fully realized under the partnership of the government and the private sector investors. By the same token, as it has been unresolved whether smart card readers, an indispensable hardware in the age of smart card technology, would be universally present and easily accessible for

the general citizens in countries like Taiwan and South Korea at this stage of technological development, whether a citizen would have any local control on his or her own personal information seems a legitimate worry.

As digital information allows perfect duplication, quick searching and efficient data transfer, introducing a national electronic ID might be quite equal to a privacy nightmare. Under the scheme, huge electronic databases which would include almost all kinds of personal information could easily be copied, stored, searched, transferred and even manipulated. Looked at in this way, digitized fingerprints stored in the smart card, as proposed in the Taiwanese project, for example, could become a real danger. For many people, furthermore, biometrics are highly intrusive and considered a typical violation of privacy which also became an issue in Taiwan's smart card ID debate.

The authority in charge of implementing Taiwan's all-in-one smart card based ID card system explained that the multi-purpose national ID scheme is attractive because it has the advantage of sharing costs across government agencies and even commercial organizations. However, as noted by an ID card expert, multi-purpose national identification schemes represents the most substantial threat of information technologies to individual liberties [10]. The fact that the government is completely ignorant of the public policy implications of the multi-purpose smart card based national ID scheme is fatal to the legitimacy of the project.

Consider just another possibility the smart card could do to a citizen in Taiwan under the future national ID regime. While with the help of smart cards people would be able to carry their money around in "electronic purse", it is also ironically true that the advantages of anonymity would not be brought to us by the convenient electronic purse under the national ID regime [17]. Theoretically, every detail of your daily lives would be easily recorded coordinately by the private and public sectors under the commercialized one-card-does-all national ID regime. Under this context, the mandatory nature of the smart card based national ID card implies that nobody would be able to choose to be anonymous, both in the real world and in the virtual world, any more. It would be unimaginable and unbearable for many people to have their lives governed by such a perfect technological architecture under which they have no escape at all.

5. Governmental Information Systems: From Outsourcing to Build-Operate-Own

Outsourcing government services is not uncommon at all in today's world. For various economic reasons, information technology related industries around the world have been competing to contract with government agencies on government databases and taking over the responsibilities for running traditional governmental services. For instance, Electronic Data Systems (EDS) in British, one of the world's largest outsourcers, plays a leading role in the outsourcing of government services in UK [13].

One of the most prominent characteristics of the smart card based national ID project in Taiwan is its proposed build-operate-own (BOO) strategy. The gist of the BOO strategy is each of the governmental agencies involved in the smart card based national ID project would not have any dedicated budget for it. Rather, in return for their investment in such project, the private company is allowed to run value-added business derived from maintaining and operating the governmental information systems. A BOO strategy is also different from the more well known build-operate-transfer (BOT) business model in that the private company may even obtain a license from the government to run the system indefinitely. In other words, the original plan of the project anticipated private sector investments to become the driving force in helping build its electronic government and promote the electronic commerce.

Moreover, although one major revenue incentive in the Taiwanese project is to permit the private BOO contractor to collect fees from citizens for government services, it is a popular prediction that the anticipated additional follow-on business opportunities under the national smart card regime are far more lucrative. For instance, the certificate authorization function of the smart card project would offer opportunities to vendors of digital signature technologies. As the government in Taiwan is currently making every effort to promote the idea and architecture of "electronic government" and electronic commerce, the electronic signature authorized for the smart card would be applied not only to personal identifications but also to all the electronic transactions conducted both in the public and private sectors.

Similarly, a legislative bill authorizing a project which is to combine all medical

records, family trees and assorted genetic information into a single computerized database with the help of deCODE Genetics, an Icelandic biotechnology company funded by venture capital, was put into serious consideration by Iceland's parliament in late 1998 and voted into a law in early 1999 [2, 14, 25]. The Iceland government will grant deCODE Genetics excluded rights to operate the health sector database for 12 years. The company can generate business from the database for diseases research, new drug development and test, and insurance application, among others.

Consider the implications of Taiwan's BOO strategy and the Iceland project. It is apparent that both governments would not have to bear the costs of building the infrastructure of the systems and their maintenance. Particularly under the BOO regime, the building and maintenance of the systems would be undertaken by the commercial consortium in exchange for exclusive rights of operating the system and the provision of value-added services associated with the system. It is true that the projects described above are not related at all and are different both in their natures and purposes to some extent. It is also true, however, that both projects involve commercial uses of huge bulk of personal information that were originally collected and controlled by public sector agencies and not accessible for commercial processing by the private sector.

It is therefore not difficult at all to understand why private sector investors would grasp the rare opportunity to take advantage of the free use of the existing governmental databases and rush to contract with government agencies under various terms. For instance, the Taiwanese project is based on a national computerized resident administration system, a national ID scheme, and a national health insurance scheme. According to the current resident administration regulations in Taiwan, a Taiwanese should carry his/her ID card all the time. At this point, it seems more than clear that the vision brought us by the multi-purpose smart card based national ID system is a prosperous e-commerce society built upon an electronic government who governs its 22 million law-abiding citizens. At the same time, projects like the creation of a comprehensive health sector database by linking the information a biotechnology company, such as deCODE, has collected with a national database of medical records would prove to be very attractive not only for the private sector's R&D, but also for government health care policymaking.

What seems equally controversial is whether the Taiwanese BOO initiative would be a sensible choice for a government positioned in the information age. Here are but three arguments against the initiative. First, smart card technologies involve a wide range of variables such as standards, chip fabrication, fingerprint recognition, system security, card readers, information content and format, application functions, system integrations, and social impacts. In Taiwan, only some of the required technologies are available locally, and many others would require active foreign participation. Reconsider the government's insistence that the smart card based national ID scheme would elevate the technological level of local industries. It seems uncertain to us that a more incentive environment for local information industries would be created by the BOO strategy.

Second, our sense is that there should be some alternatives for a better health care cost-benefit control, and thus it seems quite doubtful whether the proposed multi-purpose smart card scheme would be the only cure for the failing cost management of Taiwan's health care system. Even though a smart card based health certificate scheme can be a very effective auditing tool for health care cost control, a multi-purpose national ID scheme is not necessarily the indispensable solution.

Third, since rarely put under public scrutiny, the BOO initiative might be the quietest government privatization project in Taiwan's history, and in which no accountability problems have even been seriously considered. Aside from the unprecedented political accountability implications, these technology and efficiency oriented projects also bring about serious privacy and security worries for a half-grown constitutional democracy like Taiwan.

6. Commercial Exploitation of Citizen Databanks: An Emerging Danger?

It is hard to tell whether allowing the national ID scheme to be piggybacked as a smart card based e-commerce vehicle, and giving out exclusive rights to compile an entire population's medical and genelogical records for commercial purposes, are merely isolated incidents, or more garish examples in human history will emerge soon. Here is another example: It has been reported that a company, Image Data LLC [21], has been

buying the entire collections of driver license photographs from several US states [1, 28]. The photos are used by the company to build a fraud-protection device so that store clerks can verify the identity of a consumer by using a driver's license number or SSN to call up a digital photograph. Need not to say, the sales have raised serious privacy concerns.

These governmental citizen databanks are originally set up for specific administration purposes, but are increasingly evaluated and exploited for their commercial potential. Their commercial utilization gives rise to some controversies, and we should give an analysis on the commercial interests, legal perspectives, and ethical issues of such usage.

Comprehensive coverage of the target population is, probably, the primary reason why commercial interests are eager to access the government's citizen databanks. Take driver license photo as an example. It is infeasible for a company to collect every photo of the adult population. However, since the adult population mostly overlaps with the driving public, it makes sense to try to access the government's collection of driver license photos. Such access, if succeed, can provide legitimate and economical source of personal data that are otherwise impossible to collect. Other benefits include high quality data source (governmental databanks contain few data noise) and precise personal identification (if not explicitly anonymized during the acquisition process). The company can also ask the government for a one-time contract so that it not only gets exclusive rights for the access, but need not obtain individual agreement with each involved citizen either. New entries to the databanks can also be arranged to transfer to the company automatically.

Consider the question whether the government would be allowed to exploit its citizen databanks for any commercial value. Should it not allowed, even if it is for the citizen's own good, and has taken privacy issues (such as proper anonymization) into consideration? When one looks into related legislation for definite answers to the above questions, one often finds ambiguity. For example, Taiwan's *Computer Processing of Personal Data Act* requires the government to state the purpose of personal data collection, and to obtain authorization from the individual involved, before it can proceed. Also, the collected data can only be processed for the stated purpose. However, if

mandated by law, then the government can proceed to collect personal data without individual consent. Governmental citizen databanks can also be used for purposes other than those originally stated, as long as such usage is for academic research or public interests, among others. To avoid ambiguity and to obtain authorization, governments can resort to legislation when making commercial use of the databanks. For example, the Iceland Parliament voted into a law in December 1998 to authorize the creation and operation of the health database. Likewise, the sales of driver license photos in several US states were either made into a bill (Colorado) or passed as a budget provision (South Carolina). All state governments later backed off from the photo sales in reacting to public protests.

As evidenced by popular oppositions to the USA and Iceland cases described above, legislation along seems to bring little public support. One major concern is that the extent of the contract between the government and commercial company is not made clear to the public. This contract — which should detail the exact scope of the data transfer, state the terms of usage, set up auditing methods to monitor possible abuse, and so on — often is not a part of the the legislation and is negotiated afterward. The public then rightly feels that their personal data is whole-sold by the government, and they do not even know the exact condition of the sale. For example, it is not clear in the Taiwanese plan whether the business consortium operating the smart card ID system can collect personal data from one's using the ID for online transactions. Only after much public protest did the consortium say it would not do so, and offered a opt-out plan for people who don't want the e-commerce component in the ID. Likewise, the exact purpose of the Icelandic health database has not been made clear to public, and the contract with deCODE Genetics is negotiated after the bill is passed. In both the Icelandic and Taiwanese cases, there are no plan to set up independent commissions to oversee commercial operations and applications of the involved databanks.

Also, in the Iceland and USA cases, both of the operating companies adopt the default opt-in rule: One has to ask to be excluded from the plan. The proposed Taiwanese plan is compulsory: One always get the smart card based national ID. Researchers working on information privacy have long advocated the default opt-out rule, where people's explicit agreement must be received in advance in order for their personal data

to be collected and processed [22]. However, it seems that for commercial utilization of governmental databanks, default opt-in rule is the norm. Even with a default opt-in rule, there is still ambiguity about when and how one can exercise an opt-out. Often one is only allowed to exercise the opt-out at the beginning of a plan (not anytime during the plan), and once in the plan one cannot restrict the way his data is used. For dead people whose personal data is still in the government's databanks, they cannot exercise opt-out either.

A central conflict in commercial utilization of citizen databanks is that the utilization may even be harmful to the citizen while bringing no benefit to them. The Icelandic and Taiwanese plans both involve personal medical information. De-identification methods and secure computing devices have been proposed, respectively, to protect the citizen from harmful usage of their medical records. However, there exists no *a priori* trust between the commercial interests and the citizen. Furthermore, without an independent review body to enforce the security measure, it is difficult for people to believe that they are well protected. If harmful events occur, it becomes the citizens' burden to find out and prove that they are not at fault.

There is also an issues on distributing the benefit (mostly monetary) from commercial utilization of citizen databanks. These benefits mostly appear as monetary income to the government. This raises a fairness question. The databank being commercially utilized may not include all citizens. People can opt-out the plan. Then, why should money in exchange for opt-in people's personal data not be returned directly to them, but to the government and spent on all people instead. It has been argued that personal data can be brokered by an "infomediary" to the interested parties for their commercial value [19]. Indeed, the governments can be viewed as infomediaries as they utilize citizen databanks for commercial benefits.

7. Conclusion

It is nearly unquestionable that an electronic national databank has the tremendous potential to improve the effectiveness and efficiency of government administrations. This paper does not argue that digital technologies or smart card schemes should not be

adopted in Asian countries. The thesis of this paper is we should be more cautious about how to use smart card technologies. It might prove to be a ridiculous myth if we choose to focus only on the efficiency of digital technology, its potential in contributing to a more effective government, and thus a modern or better society. Unfortunately, it seems that decision-makers in both Taiwan and South Korea were not inspired or informed at all by the debates on the increasing dangers computerized national ID schemes pose to personal privacy. In addition, the governments might underestimate the fact that their educated and illuminated citizens have learned to appreciate and fight to protect the public value of personal privacy. Viewed in this way, rather than trying to introduce a sensible regulatory framework as their very first step, the governments seem a bit simple-minded to believe that collective values such as efficiency, commercial interest and technological innovation could be created in their emergent electronic commerce society simply by putting the smart card based national ID card scheme under the name of “citizen card”.

It seems the interests of the governments are compatible with that of the commerce. The cases described in this paper has shown not only some Asia governments are captive of the potential interests of electronic commerce, but also the lack of deliberations by their technocracies on the social, economic and legal implications of the information technology boom. Even if the governments decided to introduce the smart card based national ID scheme, its mandatory nature should be questioned and reconsidered so that an individual could exercise minimum local control and decide what information about him or her should be made known to others. Otherwise, it might become a very disturbing and controversial issue under the test of the European Union Directive on Data Privacy, one of the most important movement addressing privacy as a global matter [33] and put these Asian countries in the danger of turning themselves into isolated islands in the ocean of global information flow.

In other words, our sense is that if we want to create a marketplace for electronic commerce, we need to think over as to under what kind of architecture the marketplace of electronic commerce would work better, if not best. By the same token, if we want to argue that we should leave technological innovations alone, we need an argument about why it is right to leave technological innovations alone. Before we have a great argument

about the future technological and legal architecture of electronic commerce, our suggestion is that public values such as privacy protection should be preserved in constitutional democracies, no matter how immature they are now. Moreover, it will soon be proved to the governments in Asia that preserving these public values contributes to electronic commerce significantly in the long run. To achieve the aims, a sensible regulatory framework is indispensable and the law should regulate in public interests.

8. Notes

This article is our reflection of the public campaign against the Taiwan government's plan to transform our current national ID system to a smart card based scheme. The views expressed in this article are those of the authors and do not necessarily represent those of Academia Sinica and Tamkang University.

We are grateful to many people who contribute their time and energy in the campaign. We would like to thank Taiwan Association for Human Rights, in particular its president B. H. "Peter" Ng, for coordinating the campaign. Legislator Sun-Lu Fan has expressed her continuous concern and support for this campaign, and chaired several public hearings. We also thank our colleagues at the Institute of Information Science, Academia Sinica, for many helpful discussions.

References

[1] Special report: Image data. *The Post and Courier*. <http://www.charleston.net/news/imagedata>.

[2] A genetic argument in Iceland. *The Economist*, pages 109–110, December 5th - 11th, 1998.

[3] Rebar cancels national “smart” ID card project. *China News*, November 29, 1998. <http://www.gsn.gov.tw/eng/iccard/news8711/1129021.gif>.

[4] Use of electronic ID cards delayed. *Korea Herald*, September 25, 1998. <http://203.227.225.12/news/1998/09/__02/19980925_0211.html>.

[5] Plastic ID cards to replace current laminated ones. *Korea Herald*, February 24, 1999. <http://203.227.225.12/news/1999/02/__02/19990224_0221.html>.

[6] Catherine Allen and William J. Barr, editors. *Smart Cards: Seizing Strategic Business Opportunities*. Irwin Professional Publishing, 1996.

[7] Ross Anderson and Markus Kuhn. Low cost attacks on tamper resistant devices. <http://www.cl.cam.ac.uk/ftp/users/rja14/tamper2.ps.gz>.

[8] Ross Anderson and Markus Kuhn. Tamper resistance — a cautionary note. In *The Second USENIX Workshop on Electronic Commerce*, pages 18–21. Oakland, California, USA, November 1996. <http://www.cl.cam.ac.uk/users/rja14/tamper.html>.

[9] Nes Barrameda. SC thrashes FVR’s nat’l ID system. *The Manila Times*, July 24, 1998.

[10] Roger Clarke. Chip-based ID: Promise and peril. <http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html>.

[11] Roger Clarke. Roger Clarke’s dataveillance and information privacy pages. <http://www.anu.edu.au/people/Roger.Clarke/DV>.

[12] Lloyd Darlington. Banking without boundaries: How the banking industry is transforming itself for the digital age. In Don Tapscott, Alex Lowy, and David Ticoll, editors, *Blueprint to the Digital Economy: Creating Wealth in the Era of E-Business*, pages 113–129. McGraw–Hill, 1998.

[13] Simon Davies. Outsourcing big brother: A look behind EDS’ takeover of the UK government. <http://www.privacy.org/pi/issues/outsourcing/eds.html>.

[14] deCODE Genetics Inc. A centralised Icelandic healthcare database: Overview. <http://www.database.is/rm_almennt.html>.

[15] Dorothy E. Denning. *Information Warfare and Security*. Addison-Wesley, 1998.

[16] David H. Flaherty. *Protecting Privacy in Surveillance Societies : The Federal Republic of Germany, Sweden, France, Canada and the United States*. University of North Carolina Press, 1992.

[17] A. Michael Froomkin. Flood control on the information ocean: Living with anonymity, digital cash, and distributed databases. *Journal of Law and Commerce*, 15, 1996.

[18] Oscar H. Gandy Jr. *The Panoptic Sort: A Political Economy of Personal Information*. Westview Press, 1993.

[19] John Hagel and Marc Singer. *Net Worth: Shaping Markets When Customers Make the Rules*. Harvard Business School Press, 1999.

[20] Jan–Ming Ho, Da–Wei Wang, Shih–Kun Huang, Tyng–Ruey Chuang, Ching–Yi

Liu, and Jeng–Ran Chen. Citizen card: The worst nightmare of an information society. *China Times*, page 11, August 18, 1998. (In Chinese).
[21] Image Data LLC. <http://www.imagedatallc.com>.
[22] Jerry Kang. Information privacy in cyberspace transactions. *Stanford Law Review*, 50:1193–1294, April 1998.
[23] Korean NGO Task Force against Electronic National ID Card. No! Electronic National ID Card and Protect Personal Privacy in Korea [sic]. <http://kpd.sing-kr.org/idcard/main-e.html>.
[24] Ching–Yi Liu. Intelligent national ID: Convenience or convenient thinking. *China Times*, page 11, February 12, 1998. (In Chinese).
[25] MANNVERND. The health-sector database plans in Iceland. <http://www.simnet.is/mannvernd/english/index.html>.
[26] William H. Minor. Identity cards and databases in health care: The need for federal privacy protection. *Columbia Journal of Law and Social Problems*, 28, 1995.
[27] Multimedia Development Corporation. National multipurpose card. <http://www.mdc.com.my/flagship/card>.
[28] Lisa Napoli. 3 states curb sale of driver license photos as security device. *The New York Times*, February 4, 1999.
[29] Popular Alliance against the National IC Card System. FACT SHEET: The Proposed National IC Card System in Taiwan, October 1998. <http://nature.csie.ntu.edu.tw/~nonid/analysis_paper/fact_sheet.html>.
[30] Dexter Roberts and Bruce Einhorn. Asia logs on. *Business Week*, page 22, February 1 1999.
[31] Steering Committee for Information Development and Promotion. Request for Proposal for IC Card with Combined National ID and Health Insurance Card Functions (Citizen's Card), June 1998. <http://www.gsn.gov.tw/eng/iccard/erfp0610.html>.
[32] Sheryl Gay Stolberg. Health identifier for all Americans runs into hurdle. *The new York Times*, page A1, July 20, 1998.
[33] Peter P. Swire and Robert E. Litan, editors. *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*. Brookings Institute, 1998.

ID cards and eID initiatives: a wealth of best practices to share. Thales is contributing to 40 national eID programsÂ The idea of a National ID card that is valid for both the physical and digital domains has become a reality for millions of people. In some countries, citizens, public and private organizations are starting to reap benefits. We investigated in our recent report what are these so-called digital dividends .Â Multi-application national ID cards. Thales Gemalto MultiApp ID is a Global Platform smart card solution for eID, eDriving License, eRegistration Certificate, and eHealthcare. It is a Public Key Java Card designed to meet the most advanced security requirements of long-term multi-application programs such as the ones launched by governments and health insurance initiatives. As a candidate in 2016, Donald Trump built his argument for the presidency around his claimed acumen as a dealmaker. As the 2020 election draws nearer, President Trump and his surrogates are doubling down on that assertion, including by calling attention to what he has deemed â€œthe biggest deal ever seenâ€: the â€œphase oneâ€ trade deal with China. The agreement reportedly includes a Chinese commitment to purchase an additional $200 billion in American goods above 2017 levels by the end of 2021. Ryan Hass. Senior Fellow - Foreign Policy, Center for East Asia Policy Studies, John L. Thornton China Center. The Michael H. Armacost Chair. Chen-Fu and Cecilia Yen Koo Chair in Taiwan Studies. Nonresident Fellow, Paul Tsai China Center, Yale Law School. Ryanl_hass. To Trade or Not to Trade?: Thoughts on the Failed Smart Card Based National ID Initiative in Taiwan. June 1999. Tyng--ruey Chuang.Â Based upon an account as to how the smart card based national ID system projects in Taiwan and South Korea failed to succeed under strong protests, this paper elaborates why the scheme seems to become a particularly favored strategy for some Asian governments, especially those who already have national ID card systems in place for several decades, to adopt in vitalizing or escalat... Based on the Supreme Court docket of India, there is no such thing as a authorized, substantial foundation to impose strict restrictions on cryptocurrencies, in the mean time. However as soon as the regulation is handed within the parliament, the Supreme Court docket is not going to have a say on this matter. On account of this uncertainty, banks are advising the residents to not commerce cryptocurrencies. The Centre is contemplating a proposal to ban or restrict the attain and accessibility of cryptocurrencies and launching their very own digital tokens to assist the safe, digital cost motion... The OBOR initiative is expected to deepen economic relations between China and other countries, and will also raise Chinaâ€™s position on the world stage, thus making it possible for the largest emerging economy to acquire a bigger say in making the international rules. This is particularly inevitable as the Transatlantic Trade and Investment Partnership (TTIP) and the Trans-Pacific Partnership (TPP), which exclude China, Russia and many others, are going to play an important role in setting â€œnew rules for a new eraâ€. It is believed that, by implementing the OBOR initiative, China and other coun...