Towards a National ID System: An Examination of Kilusang Mayo Uno, et al. v. the Director General and Executive Order No. 420

André Ria B. Buzeta-Acero[*]

I. INTRODUCTION 149
II. FACTS OF THE CASE 151
III. LEGISLATIVE HISTORY 152
IV. WHAT IS A NATIONAL ID SYSTEM? 156
V. TREND TOWARDS NATIONAL ID SYSTEMS 158
A. United States
B. United Kingdom and Europe
C. Australasia
VI. LEGAL ARGUMENTS 161
A. The right to privacy
B. Arguments in favor of a National ID System
C. Arguments against a National ID System
VII. CASE LAW 173
A. Whalen v. Roe
B. Ople v. Torres
VIII. A CRITIQUE OF E.O. 420 175
Does E.O. 420 establish a National ID System?
IX. E.O. 420 AND THE RIGHT TO PRIVACY 176
X. CONCLUSION 181

I. INTRODUCTION

One of the inherent challenges of running a government is how to maximize efficiency and minimize costs. Good governance means not only providing basic social services but making sure that these services are aptly and competently delivered. One of the ways for government to enhance the

* '07 J.D. cand., Ateneo de Manila University School of Law; Member, Board of Editors, *Ateneo Law Journal*. The author would like to thank Francis Euston R. Acero whose invaluable help, support, intelligence and research skills, made the completion of this case comment possible.

Cite as 51 ATENEO L.J. 149 (2006).

integrity and reliability of its transactions is to reduce unnecessary and costly redundancies by devising tools to simplify complicated government operations.

The Arroyo government's recent move for a unified identification system with Executive Order No. 420 (E.O. 420)[1] prompts to serve as a device to increase efficiency in government operations and transactions. This bid for a unified identification system recognizes that the existing multiple identification systems have created unnecessary redundancies and higher costs to the government. It intends to facilitate private businesses, enhance the integrity and reliability of government-issued identification cards in private transactions, and prevent violations of laws involving false names and identities.[2]

The Supreme Court recently upheld the constitutionality of E.O. 420 and pointed out that unified data collection and recording in government entities would achieve substantial benefits. The Supreme Court further said that "the right to privacy does not bar the adoption of reasonable identification systems for government entities."[3]

The institution of a National Identification System (National ID System) or a similar Integrated Identification System has always been a contentious issue, not only in the Philippines, but also around the globe. Civil libertarians, human rights advocates, and militant groups have long claimed that the institution of a National ID System violates a citizen's intrinsic right to privacy and could easily be used and abused by the government to keep track of a person's private activities.[4]

The arguments against E.O. 420 are similarly inclined, and despite the Supreme Court's stamp of approval, there is still staunch opposition against the implementation of the executive order because the Supreme Court's decision did not thoroughly deliberate on the civil rights issues and the many repercussions of having an integrated national identification system, but merely discussed the procedural validity of the creation of the executive order. The issue surrounding the recent decision of the Supreme Court

1. Requiring All Government Agencies and Government-Owned And Controlled Corporations to Streamline and Harmonize their Identification (ID) Systems, and Authorizing for such Purpose the Director-General, National Economic and Development Authority to Implement the Same, and for other Purposes, Executive Order No. 420 [E.O. 420] (2005).

2. *Id.*

3. Kilusang Mayo Uno, et al., v. the Director-General, et al., G.R. No. 167798, April 19, 2006.

4. Senate Economic Planning Office Policy Insights, *National Identification System: Do We Need One?* (2005).

declaring E.O. 420 constitutional and its subsequent implementation strikes at the very core of a citizen's relationship with the State, hence, merits discussion.

The first part of this paper discusses the concept of an Integrated or National ID System. The second part then focuses on the Philippine experience with regard to attempts in setting up a National ID System. In the final section, this paper discusses the present decision in light of judicial precedent regarding the right to privacy and the implementation of a national identification system – looking at distinctions that may exist between the present case of *Kilusang Mayo Uno, et al., v. the Director General, et al.* and previous attempts at an integrated identification system.

II. FACTS OF THE CASE

With the seemingly noble goal of cutting red tape and improving government efficiency, President Gloria Macapagal Arroyo recently issued Executive Order No. 420 seeking to start the implementation of a unified multi-purpose identification system by "harmonizing" the identification systems of government agencies, including government-controlled corporations.[5]

Under this Unified Identification System, government agencies will collect three kinds of data: basic, biometric, and other information. Basic data will comprise a person's name, date and place of birth, name of parents, and gender. Biometric data will consist of the individual's photograph, signature, and prints of the index fingers and thumbs. Other data will include the individual's specific home address, marital status, height, weight, prominent distinguishing features, and his Tax Identification Number.[6]

The constitutionality of E.O. 420 was questioned in two petitions filed by Kilusang Mayo Uno and Bayan Muna sectoral representatives led by Satur C. Ocampo. Both petitions raised two major issues, namely that: (1) E.O. 420 is a usurpation of legislative functions, and (2) it infringes on the citizen's right to privacy.[7]

In the full-court decision last 19 April 2006, penned by Justice Antonio T. Carpio, the Supreme Court upheld the constitutionality of E.O. 420. The Supreme Court ruled that "E.O. 420 applies only to government entities that already maintain ID systems and issue ID cards pursuant to their regular functions under existing laws. E.O. 420 does not grant such government entities any power that they do not already possess under existing laws." The

5. *Id.*

6. *Id.*

7. *Kilusang Mayo Uno, et al.*, G.R. No. 167798.

Supreme Court held that E.O. 420 applies only to the Executive branch of government and "does not extend to the judiciary or to the independent constitutional commissions," and that "in the present case, E.O. 420 does not establish a National ID System but makes the existing sectoral card systems of government entities less costly, more efficient, reliable, and user-friendly to the public." Hence, the Supreme Court ruled that "E.O. 420 is a proper subject of executive issuance under the President's constitutional power of control over government entities in the Executive department, as well as under the President's constitutional duty to ensure that laws are faithfully executed."

The Supreme Court also differentiated E.O. 420 from Administrative Order No. 308[8] (A.O. 308) issued by then President Fidel V. Ramos in 1996 that called for the setting up of a National Computerized Identification Reference System, as that power did not exist prior to the issuance of the assailed executive directive. The Supreme Court nullified A.O. 308 in 1998 because it seeks to create "a new national data collection and card issuance system where none existed before."

III. LEGISLATIVE HISTORY

In the Philippines, attempts to establish a National ID System started during the martial law years under the regime of former President Ferdinand E. Marcos and was unabashedly proposed as part of the government's counter insurgency program. President Marcos issued Presidential Decree No. 278[9] (P.D. 278). However, P.D. 278 remained unimplemented on a national scale for reasons still undisclosed.

In 1982, Rodolfo Albano, then serving as a member of the Batasang Pambansa, revived the idea of having a National ID System. The same bill was re-filed 10 years later but it never caught on as the political opposition raised the possibility that the idea might possibly be violative of human rights.[10] In 1988[11] and 1991,[12] the Philippine Senate and House of Representatives, in separate moves, attempted to establish such a National

8. Adoption of a National Computerized Identification Reference System, Administrative Order No. 308 [A.O. 308] (1996).

9. Instituting a National Reference Card System and Creating Therefore The National Registration Coordinating Committee, Presidential Decree 278 [P.D. 278] (1973).

10. Jaime C. N. Arroyo, Resurrection of National ID System Legislation Proposed, June 21, 2001, http://www.cyberdyaryo.com/ features/ f2001_0621_02.htm (last accessed May 15, 2006).

11. *See* House Bills No. 2124, 5006, 5130, 4953 and 5603.

12. *See* Senate Bills no. 1547 and 1685.

ID System, which downplayed the reason of national security and highlighted alleged conveniences to be gained by the implementation of such an ID system.

The 10th Congress saw three separate bills being filed reviving the idea of a national ID system. The first was filed on 31 July 1995 by Representative Charito B. Plaza of the 1st District of Agusan del Norte as House Bill No. 374. The bill hoped to facilitate government transactions, prevent election fraud, and help solve crimes.[13] The second, House Bill No. 6335, on the other hand, filed by Representative Roger Mercado of the lone district of Southern Leyte on 22 February 1996, hoped to reduce red tape and facilitate transactions ranging from taxpaying to marriage, and also to enable the government to monitor criminal activity.[14] The third bill, House Bill No. 8530, was principally authored by Representative Santiago Respicio with the help of Representatives Antonio Abaya, Faustino Dy, and Rodolfo Albano, also hoped to facilitate contractual transactions, combat red tape, and combat terrorism and preserve national security.[15]

Under House Bill No. 374, the information in the identification card to be issued included an individual's name, age, date and place of birth, citizenship, his spouse's and parents' names, his residences both permanent and temporary, occupation, and such additional matters which would be required by the local civil registrar, together with passport-sized photographs. The said identification card was supposed to be issued to Filipinos upon reaching the age of majority and each person would also be assigned a permanent, non-transferable identification number.[16]

In House Bill No. 6335, there was an enumeration of the circumstances under which the bearer of the identification card would be required to present it. These included:

a. acknowledgment of a document before a notary public,

b. taking of an oath of office,

c. receipt of a license, certificate or permit from any public authority, and

d. payment of taxes.[17]

---

13. Arroyo, *supra* note 10.

14. *Id.*

15. *Id.*

16. *Id.*

17. *Id.*

However, under House Bill No. 6335, there was no mention of the contents of the ID, but it was only said that Filipinos and resident aliens over 18 years of age would be issued a card and assigned a permanent, non-transferable number. The bill's failure to detail what kind of information would be included in the said ID ensured its lack of support in the Lower House. None of these bills made it past the first reading.

Carving a snake another way, Senator Miriam Defensor-Santiago proposed the creation of a national crime database, which some pundits considered to be similar to a national ID system,[18] thus dooming the proposal. It likewise did not pass first reading in the Senate.

Arguably, the most controversial attempt at creating a national ID system occurred during the Ramos administration, when he issued A.O. 308. The said order mandated that certain government agencies contribute data toward the creation of a national database, from which people would be assigned a certain Population Reference Number generated by the National Statistics Office. In addition, the database would also make reference to a person's biometrics, which Justice Reynato Puno in his decision defined as "the science of the application of statistical methods to biological facts; a mathematical analysis of biological data."[19]

Biometric systems are automated, mostly computerized systems using distinctive physio-biological or behavioural measurements of the human body that serve as a (supposedly) unique indicator of the presence of a particular individual.[20] Justice Puno also noted that "[t]oday, biometrics is no longer limited to the use of fingerprint to identify an individual. It is a new science that uses various technologies in encoding any and all biological characteristics of an individual for identification."[21]

Civil society groups, and concerned citizens, including the late Senator Blas Ople, opposed the implementation of A.O. 308 on the ground of its unconstitutionality, as it was a usurpation of legislative power and an invasion of a person's privacy. This contention was sustained by the Supreme Court, and will be discussed later in this paper in the light of the present decision.[22] At present, there are several bills pending with the House of

18. *Id.* (Defensor-Santiago's bill did not actually propose an all-encompassing national ID system; the proposal was limited to the creation of a database of all individuals with criminal records.).

19. *See* Ople v. Torres, 293 SCRA 141 (1998).

20. Canadian Internet Policy and and Public Interest Clinic, Biometrics FAQs, *at* http://www.cippic.ca/en/faqs-resources/biometrics/ (last accessed May 17, 2006).

21. *Ople*, 293 SCRA at 160.

22. *Id.* at 144.

Representative's Committee on Justice[23] dealing with the establishment of a National ID System.

Representative Rozzano Biazon, of the lone district of Muntinlupa, filed House Bill No. 217.[24] The bill seeks to establish an identification system in the Philippines with the aim of reaping the same benefits as those achieved in the countries like Malaysia, Indonesia, Japan, Germany, and South Africa, where the adoption of an identification system has provided a useful tool in minimizing, if not eradicating, bureaucratic red tape. Similarly, House Bill No. 1244[25] was filed by Representative Eduardo Veloso, which seeks to establish and maintain a complete, adequate and consolidated National ID to attain the following objectives: 1) to streamline and economize the bureaucracy by consolidating the present ID systems with the National ID system; 2) to facilitate and expedite statistical data gathering by pertinent government institutions; and 3) to provide Filipino citizens with a simple and effective identification system to conduct transactions.

House Bill No. 3768[26] filed by Representative Gilbert Remulla also seeks to establish a national identification system to preserve national security and expedite private and public transactions.

House Bill No. 3433[27] filed by Representative Anthony Miranda mandates any person residing in the Philippines to apply for registration and issuance of an identification card with a permanent serial number at the office of the Local Civil Registrar.

House Bill No. 2620[28] filed by representative Amado Espino, on the other hand, seeks to provide for a tamper-proof National ID (NID) Card which may be used to transact with any government instrumentality without need of further proof as to an individual's identity.

---

23. *See* The Congress of the Philippines, 13th Congress, Committee on Justice, *at* http://www.congress.gov.ph/committees/ (last accessed May 16, 2006).

24. An Act Establishing a Mechanism for the National Identification System in the Philippines, Providing for Benefits and Rights and Corresponding Obligations, and for other Purposes, House Bill No. 217 filed on July 1, 2004.

25. An Act Providing for the Establishment of a National Identification (ID) System to Consolidate Existing ID Systems and Appropriating Funds Therefor, House Bill No. 1244, filed on July 7, 2004.

26. An Act Providing for a National Identification System, Defining its Coverage and Appropriating Funds Therefor, and for other Purposes, House Bill No. 3768, filed on Feb. 21, 2005.

27. An Act Providing for a National Identification System and Appropriating Funds Therefor, and for other Purposes, House Bill No. 3433, filed on Dec. 7, 2004.

28. An Act Establishing a National Identification System (NIDS) in the Philippines, House Bill No. 2620, filed on Aug. 24, 2004.

House Bill No. 3825[29] filed by Representative Faysah Maniri-Racman Dumarpa, proposes the adoption of a national identification system that shall serve as the official identification card of Filipino citizens and alien permanent residents when dealing with all government institutions.

Representative Prospero Pichay, Jr. also proposed a bill providing for the establishment of a Philippine citizenship identification system,[30] which requires all Filipino citizens, who have reached the age of majority, to secure a citizen's ID from the Bureau of Immigration.

In the Senate, Senator Aquilino Pimentel filed Senate Bill No. 1138.[31] The bill intends to facilitate the issuance of passports and other official documents from the government and seeks to make the payment of fees and the collection of taxes much easier and more efficient. It also aims to eliminate election fraud.

IV. WHAT IS A NATIONAL ID SYSTEM?

A National ID System is generally an instrument used by governments to assist public agencies in identifying and verifying the identities of citizens who are availing of government services or making public transactions.[32]

In general, there are three types of National ID Systems, namely: (1) Stand Alone System; (2) Registration System; and (3) Integrated System.[33] Stand Alone ID cards are usually issued by governments undergoing political transitions, such as military or emergency rule, or in environments which are subject to sudden economic or political change. Under the Registration System, the ID card contains information that is stored in a registration system managed by a government agency. In an Integrated System, a card number is usually assigned to an individual as a form of identifier. Several government agencies form part of the integrated system.[34] Virtually all card systems established in the past 10 years are integrated systems.[35]

---

29. An Act Establishing the Philippine National Identification System, House Bill No. 3825, filed on Feb. 28, 2005.

30. An Act Providing for the Establishment of a Philippine Citizenship Identification System, House Bill No. 748, filed on July 27, 2004.

31. An Act Establishing the Philippine National Identification System, Senate Bill No. 1138, introduced on Sept. 7, 2004.

32. *National Identification System: Do We Need One?, supra* note 4, at 1.

33. Privacy International. Identity Cards, Frequently Asked Questions, August 24, 1996, *at* http://www.privacy.org/pi/activities/idcard/idcard_faq.html#1 (last accessed May 17, 2006).

34. *Id.*

35. *Id.*

The concept of an integrated national identification system was first instituted in countries with populations coming from diverse ethnic groups.[36] The basic idea was to generally use the ID card as a means of identifying people of a certain race, politics or religion.[37] In fact, as critics of ID cards occasionally point out, some countries, such as Germany and Spain, introduced the cards under fascist regimes in the 1930's and have not withdrawn them.[38]

During World War II, a national ID card was established in the United Kingdom to facilitate identification of aliens. Persons were required to carry the card at all times and show it to police and members of the armed forces on demand.[39] In 1951, Acting Lord Chief Justice Lord Goddard ruled that police demanding that individuals show their ID cards was unlawful because it was not relevant to the purposes for which the card was adopted. This ruling led to the repealing of the National Registration Act and the end of the national ID card in the United Kingdom in 1952.[40]

At present, several countries, rich and poor alike, are implementing a national ID system. They include Belgium, Germany, Greece, Italy, Poland, and Spain. Interestingly, none of the major common law countries such as the United States, Canada, United Kingdom, Australia and New Zealand has a national ID card regime.[41] However, in recent years there has been an increase in interest in these countries to institute national ID cards and they are currently investigating possible ways of introducing either voluntary or mandatory ID cards.

The type of card, its purpose and the information it contains, vary from country to country.[42] For most countries, the information in identification

---

36. *Id.*

37. Jim Fussell, Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing, Prevent Genocide International, Nov. 15, 2001 *at* http://www.preventgenocide.org/prevent/removing- facilitating-factors/IDcards (last accessed May 17, 2006).

38. Mark Watkins, National ID Cards, FAQs and Resources, Canadian Internet Policy and Public Interest Clinic, *at* http://www.cippic.ca/en/faqs-resources/national-id-cards (last accessed May 17, 2006).

39. Privacy International, History of ID Cards in the United Kingdom, January 1, 1997, *at* http://www. privacyinternational.org (last accessed May 17, 2006).

40. *Id.*

41. *Id.*

42. Tova Andrea Wang, The Century Foundation Homeland Security Project, The Debate Over a National Identification Card, May 10, 2002, *at* http://www.tcf.org/Publications/HomelandSecurity/National_ID_Card.pdf (last accessed May 15, 2006).

cards is similar to information that one may find in an ordinary credit or any employment ID card. The amount of information and the kind of data contained in the cards depend on the purpose for which it is intended to be used. In Belgium, the ID is used by citizens as proof of age when purchasing liquor and going to places meant "for adults-only."[43]

One of the main purposes of having an integrated or national ID card is for identification purposes. A national ID card as a general identification document could be used in many different situations, both in dealing with government agencies and private entities.[44] One of the main goals of introducing a national ID card is the so-called *synergy effect* of replacing multiple identification documents with a single, standardized, and widely recognized document.[45] An integrated ID card could help in facilitating the delivery of basic services and authenticate their entitlement to such servces, including benefits derived from social legislation. It would also improve the much-maligned inefficiency of government. Instead of presenting authenticated copies of documents that may take weeks or in some circumstances, even months to procure, the presentation of an integrated ID card would shorten this already-tedious procedure.

V. TREND TOWARDS NATIONAL ID SYSTEMS

A. United States

For the longest time, the United States has traditionally been resistant to the idea of a National ID System. Sectors who were concerned of its possible use to invade the privacy of its citizens made sure that the idea, grounded on the expansion of their social security number system, never gained much support. However, as a result of the September 11 attack, the public outcry against invasions to privacy waned and the public grew more receptive to the idea of an integrated database of information in the name of national security.[46] Lingering concerns on privacy[47] meant that in the Patriot Act of

43. *Id.*

44. Biometrics FAQs, *supra* note 20.

45. *Id.*

46. Pew Research Center For the People and the Press, *at* http://people-press.org/ (last accessed May 15, 2006); *see also* Jennifer Jones, *Sept. 11 Attacks Stir National ID Card Debate*, INFOWORLD, Sept. 25, 2001, *available at* http://www.infoworld.com/articles/hn/xml/01/09/25/010925hnidcard.html (last accessed May 15, 2006).

47. *Id.* (Despite pronouncements on the demise of privacy as an issue with the American public, phone surveillance and the scanning of e-mail remained to be non-negotiables for a significant number of Americans.).

2001,[48] biometric technology was used on its alien and border control system, making it one of two countries, the other being the United Arab Emirates, to keep biometric technology for that purpose.[49] It would not be until May 2005 that a federal law was passed that ordered the creation of an "electronically readable,... federally approved card" for United States citizens and residents, effectively creating a standard driver's license for the entire United States by the year 2008.[50]

Critics of the act, specifically Barry Steinhardt of the American Civil Liberties Union, has been quoted as saying that "[the law] is going to result in everyone, from the 7-Eleven store to the bank and airlines, demanding to see the ID card... It's going to be not just a national ID card but a national database."[51]

B. United Kingdom and Europe

On the other side of the pond, initiatives to renew the national ID system were in place from the government of former Prime Minister John Major. As mentioned earlier, compulsory identity cards were issued during the two World Wars. It must be noted, however, that support for these identity cards waned shortly after the wars ended. The plans died with the Conservative Party's hold on power in 1997. Not even the September 11 attack could wither public outcry against such an idea. However, rising incidences of identity theft and welfare abuse led to a 2002 proposal to create "entitlement cards" which were supposed to end such abuse. In the end, and bolstered by increased terrorist activity on British soil,[52] Parliament passed the Identity Cards Act of 2006, which established a British National Identity Card linked to a national database.[53] The United Kingdom is the fifth common law country to use a national ID system in peacetime, after Cyprus, Hong Kong, Malaysia, and Singapore.

---

48. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, U.S.A. Patriot Act (2006).

49. Wikipedia, British National Identity Card, *at* http://en.wikipedia.org/wiki/British_national_identity_card (last accessed May 16, 2006).

50. *National Identification System: Do We Need One?, supra* note 4, at 4.

51. *Id.*

52. *See* Wikipedia, 7 July 2005 London Bombings, at http://en.wikipedia.org/wiki/7_July_2005_London_bombings (last accessed May 16, 2006) (On July 7, 2005, several bombs exploded simultaneously on London streets.).

53. To support the idea, the British Home Office released documentation claiming that the identity cards would generate at least £650m to £1.5bn in savings each year, among other benefits.

In July 2005 the United Kingdom indicated that it would use its six-month presidency of the European Union from July-December 2005 to promote initiatives towards a European biometric ID scheme for passports[54] following a request from the International Civil Aviation Organization (ICAO).[55] However, the proposal was met with concerns that such a policy might violate existing privacy regulations.[56]

Although 21 of the 24 European Union member-states already employ some form of identification documentation, these systems are not necessarily compulsory, biometric, or linked to a national database.[57] A majority of these systems around the European Union are paper-based and announcements on the same are only aimed at improving already existing systems, with no mention of whether or not biometrics are to be included in the upgrade.[58]

C. Australasia

In the light of the forward role played by the Australian government in response to the events of September 11, more conservative elements in the Australian parliament proposed a national identification scheme ostensibly to fight against terrorism, on the ground that citizens of first world countries are now more willing to accept stringent restrictions on civil liberties as the price of not being killed by terrorists.[59]

Malaysia's identification card scheme, however, is proving to be the most comprehensive. Founded on an anti-terrorism and increased efficiency platform, the Malaysian card, dubbed "MyKad," is set to combine one's driver's license, health maintenance organization card, prepaid toll credit,

54. *See* full text of EU Directive *at* http:// www.cdt.org/privacy/eudirective/EU_Directive_.html (last accessed May 16, 2006)(The European Union does not have any legislative power; instead, it offers policy directives toward its members. With regard to privacy, EU policy is set forth in the 1998 European Union Privacy Directive, which although aimed at corporations vis-à-vis their employees, may also well be fully appreciated to include governments.).

55. EurActiv.com, Biometric Era Raises Fears Over Privacy, *at* http://www.euractiv.com/en/justice/biometric-era-raises-fears-privacy/article-111988 (last accessed May 16, 2006).

56. *Id.*

57. *National Identification System: Do We Need One?, supra* note 4, at 4.

58. *Id.*

59. Australian Privacy Foundation. A New "Australian Card:" The Costs Outweigh the Benefits: An Open Letter to Coalition MPs., July 28, 2005, *at* http://www.privacy.org.au/Campaigns/ID_cards/NatIDScheme.html (last accessed May 16, 2006).

and an automated teller machine card all in one smart card.[60] The same report indicates that other countries in the region, such as China, India, Thailand and the Persian Gulf States are likewise considering the introduction of biometric-based identification systems.[61]

VI. LEGAL ARGUMENTS

The core legal issue in any discussion of a national ID system is whether or not the institution of a national ID system infringes one's right to privacy. To further understand the issue, a preliminary discussion on the right to privacy must be made.

A. The right to privacy

As defined in *Ople,*[62] the right to privacy is essentially the right to be let alone. Traditionally, this right is discussed together with the right to privacy of communication and correspondence enshrined in Article III, Sec. 3(1) of the 1987 Philippine Constitution:

> Sec. 3. (1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law.

However, writers are all of the opinion that the scope of the right is larger than that provided in the said provision. As such, there is no specific provision in the Bill of Rights[63] defining and encompassing the scope of the right to privacy. Instead, various facets of this right are distributed over several provisions in the Bill of Rights, to wit:

> Sec. 1. No person shall be deprived of life, liberty, or property without due process of law, nor shall any person be denied the equal protection of the laws.
>
> x x x
>
> Sec. 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the

60. Card Technology, Going Global with National I.D, *at* http://www.wired.com/news/conflict/0.2106,47073,00.html (last accessed May 17, 2006).

61. *Id.*

62. Ople v. Torres, 293 SCRA 141, 153 (1998).

63. PHIL. CONST. art III.

> complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.
>
> x x x
>
> Sec. 6. The liberty of abode and of changing the same within the limits prescribed by law shall not be impaired except upon lawful order of the court. Neither shall the right to travel be impaired except in the interest of national security, public safety, or public health, as may be provided by law.
>
> x x x
>
> Sec. 8. The right of the people, including those employed in the public and private sectors, to form unions, associations, or societies for purposes not contrary to law shall not be abridged.
>
> x x x
>
> Sec. 17. No person shall be compelled to be a witness against himself.

This right was first enunciated by the United States Supreme Court in the case of *Griswold v. Connecticut*.[64] In this case, Griswold was the Executive Director of the Planned Parenthood League of Connecticut. Both she and the Medical Director for the League gave information, instruction, and other medical advice to married couples concerning birth control. Griswold and her colleague were convicted under a Connecticut law which criminalized the provision of counselling, and other medical treatment, to married persons for purposes of preventing conception.[65]

The United States Supreme Court held that though the Constitution does not explicitly protect a general right to privacy, the various guarantees within the Bill of Rights create penumbras, or zones, that establish a right to privacy. Together, the First[66], Third[67], Fourth[68], Fifth[69] and Ninth[70]

---

64. Griswold v. Connecticut, 381 U.S. 479 (1965).

65. *Id. See also* Oyez Project *at* http://www.oyez.org/oyez/resource/case/149/ (last accessed May 15, 2006).

66. U.S. CONST. amend. I, (1791), states that:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

67. U.S. CONST. amend. III (1791), states that:

> No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

68. U.S. CONST. amend. IV (1791), states that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be

Amendments of the United States Constitution create a new constitutional right, the right to privacy in marital relations. The Connecticut statute conflicted with the exercise of this right and was therefore declared null and void.

Justice Douglas, speaking for five members of the US Supreme Court, stated:

> Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers 'in any house' in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.' The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: 'The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.'[71]

Justice Douglas referred to various American Supreme Court decisions[72] and said that, "[t]hese cases bear witness that the right of privacy which presses for recognition is a legitimate one."[73]

> violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

69. U.S. CONST. amend. V (1791), states that:

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

70. U.S. CONST. amend. IX (1791), states that:

> The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

71. Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

72. Boyd v. United States 116 U.S. 616 (1886); Breard v. City of Alexandria 341 U.S. 622 (1951); Public Utilities Comm. v. Pollak 341 U.S. 451 (1952); Frank v. Maryland 359 U.S. 360 (1959); Monroe v. Pape 365 U.S. 167 (1961); Mapp v. Ohio 367 U.S. 643 (1961); Lanza v. New York 370 U.S. 139 (1962).

Our very own Supreme Court recognized this right to privacy in the case of *Morfe v. Mutuc*.[74] In this case, the periodical submission "within the month of January of every other year thereafter"of sworn statement of assets and liabilities under Section 7 of Republic Act No. 3019,[75] after a government officer or employee had declared his financial condition upon assumption of office was challenged for being violative of due process as an oppressive exercise of police power and as an unlawful invasion of the constitutional right to privacy. The lower court ruled for the plaintiff and declared that the requirement of periodical submission of such sworn statement of assets and liabilities exceeds the permissible limit of the police power and is thus offensive to the due process clause.

The Supreme Court reversed the lower court's ruling and held that,

> The challenged statutory provision does not call for disclosure of information which infringes on the right of a person to privacy. It cannot be denied that the rational relationship such a requirement possesses with the objective of a valid statute goes very far in precluding assent to an objection of such character. This is not to say that a public officer, by virtue of the position he holds, is bereft of constitutional protection; it is only to emphasize that in subjecting him to such a further compulsory revelation of his assets and liabilities, including the statement of the amounts and sources of income, the amounts of personal and family expenses, and the amount of income taxes paid for the next preceding calendar year, there is no unconstitutional intrusion into what would otherwise be a private sphere.[76]

Speaking through the late Chief Justice Enrique Fernando, the Supreme Court adopted the *Griswold* ruling, which provided a wider implication of the right to privacy when it "invalidated a statute which made the use of contraceptives a criminal offense" on the ground that it is an unconstitutional invasion of the right of privacy of married persons. *Griswold* recognized that there is a constitutional right to privacy that has come into its own.[77] Justice Fernando went on to say that such right of privacy also exists in our jurisdiction and "the right to privacy... is accorded recognition independently of its identification with liberty... and it is fully deserving of constitutional protection."

Justice Fernando quoted Professor Emerson in justifying this stance on this pronouncement in *Morfe*:

---

73. *Griswold*, 381 U.S. at 484.

74. Morfe v. Mutuc, 22 SCRA 424 (1968).

75. Anti-Graft and Corrupt Practices Act, Republic Act No. 3019 (1960).

76. *Morfe*, 22 SCRA 424, at 445-46.

77. *Id.* at 444.

> The concept of limited government has always included the idea that governmental powers stop short of certain intrusions into the personal life of the citizen. This is indeed one of the basic distinctions between absolute and limited government. Ultimate and pervasive control of the individual, in all aspects of his life, is the hallmark of the absolute state. In contrast, a system of limited government safeguards a private sector, which belongs to the individual, firmly distinguishing it from the public sector, which the state can control. Protection of this private sector—protection, in other words, of the dignity and integrity of the individual—has become increasingly important as modern society has developed. All the forces of a technological age—industrialization, urbanization, and organization—operate to narrow the area of privacy and facilitate intrusion into it. In modern terms, the capacity to maintain and support this enclave of private life marks the difference between a democratic and a totalitarian society. [78]

Ople also notes that the right to privacy is also recognized in several statutory laws.[79] Article 26 of the Civil Code,[80] recognizes that "[e]very person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons"[81] and "punishes as actionable torts several acts by a person of meddling and prying into the privacy of another."[82] Article 32 of the Civil Code holds public officers or employees or any private individual liable for damages for directly or indirectly obstructing, defeating, violating or in any manner impeding or impairing any violation of the rights and liberties of another person.[83]

---

78. Emerson, Nine Justices in Search of a Doctrine, 64 Mich. Law Rev. 219, 229 (1965).

79. Ople v. Torres, 293 SCRA 141,157 (1998).

80. An Act to Ordain and Institute the Civil Code of the Philippines, Republic Act No. 386 [CIVIL CODE].

81. CIVIL CODE, art. 26 provides:

> Art. 26. Every person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons. The following and similar acts, though they may not constitute a criminal offense, shall produce a cause of action for damages, prevention and other relief:
>
> Prying into the privacy of another's residence;
>
> Meddling with or disturbing the private life or family relations of another;
>
> Intriguing to cause another to be alienated from his friends;
>
> Vexing or humiliating another on account of his religious beliefs, lowly station in life, place of birth, physical defect, or other personal condition.

82. *Ople*, 293 SCRA at 157.

83. CIVIL CODE, art. 32 provides:

Art. 32. Any public officer or employee, or any private individual, who directly or indirectly obstructs, defeats, violates or in any manner impedes or impairs any of the following rights and liberties of another person shall be liable to the latter for damages:

(1) Freedom of religion;

(2) Freedom of speech;

(3) Freedom to write for the press or to maintain a periodical publication;

(4) Freedom from arbitrary or illegal detention;

(5) Freedom of suffrage;

(6)The right against deprivation of property without due process of law;

(7) The right to a just compensation when private property is taken for public use;

(8) The right to the equal protection of the laws;

(9) The right to be secure in one's person, house, papers, and effects against unreasonable searches and seizures;

(10) The liberty of abode and of changing the same;

(11) The privacy of communication and correspondence;

(12) The right to become a member of associations or societies for purposes not contrary to law;

(13) The right to take part in a peaceable assembly to petition the government for redress of grievances;

(14) The right to be free from involuntary servitude in any form;

(15) The right of the accused against excessive bail;

(16) The right of the accused to be heard by himself and counsel, to be informed of the nature and cause of the accusation against him, to have a speedy and public trial, to meet the witnesses face to face, and to have compulsory process to secure the attendance of witness in his behalf;

(17) Freedom from being compelled to be a witness against one's self, or from being forced to confess guilt, or from being induced by a promise of immunity or reward to make such confession, except when the person confessing becomes a State witness;

(18) Freedom from excessive fines, or cruel and unusual punishment, unless the same is imposed or inflicted in accordance with a statute which has not been judicially declared unconstitutional; and

(19) Freedom of access to the courts.

In any of the cases referred to in this article, whether or not the defendant's act or omission constitutes a criminal offense, the aggrieved party has a right to commence an entirely separate and distinct civil

Article 723 of the Civil Code, further recognizes the privacy of letters and other private communications, unless court authorizes their publication or dissemination if the public good or the interest of justice so requires.[84]

The Revised Penal Code[85] punishes the violation of secrets by an officer with a range of penalties within *prision correcional* depending on whether such disclosure has caused serious damage to national interest.[86] It also likewise punishes the discovery of secrets through seizure of correspondence, which does not apply to "parents, guardians, or persons entrusted with the custody of minors with respect to the papers or letters of the children or minors placed under their care or study, nor to spouses with respect to the papers or

---

action for damages, and for other relief. Such civil action shall proceed independently of any criminal prosecution (if the latter be instituted), and may be proved by a preponderance of evidence.

The indemnity shall include moral damages. Exemplary damages may also be adjudicated.

The responsibility herein set forth is not demandable from a judge unless his act or omission constitutes a violation of the Penal Code or other penal statute.

84. CIVIL CODE, art. 723 provides:

> Art. 723. Letters and other private communications in writing are owned by the person to whom they are addressed and delivered, but they cannot be published or disseminated without the consent of the writer or his heirs. However, the court may authorize their publication or dissemination if the public good or the interest of justice so requires. (n).

85. An Act Revising the Penal Code and Other Penal Laws [REVISED PENAL CODE].

86. REVISED PENAL CODE, arts. 229 and 230 provide:

> Art. 229. *Revelation of secrets by an officer.* — Any public officer who shall reveal any secret known to him by reason of his official capacity, or shall wrongfully deliver papers or copies of papers of which he may have charge and which should not be published, shall suffer the penalties of prision correccional in its medium and maximum periods, perpetual special disqualification and a fine not exceeding 2,000 pesos if the revelation of such secrets or the delivery of such papers shall have caused serious damage to the public interest; otherwise, the penalties of prision correccional in its minimum period, temporary special disqualification and a fine not exceeding 50 pesos shall be imposed.
>
> Art. 230. Public officer revealing secrets of private individual. — Any public officer to whom the secrets of any private individual shall become known by reason of his office who shall reveal such secrets, shall suffer the penalties of arresto mayor and a fine not exceeding 1,000 pesos.

letters of either of them," and the revelation of trade and industrial secrets.[87] The Revised Penal Code also punishes trespass to dwelling.[88]

Justice Puno in *Ople* also noted that special laws such as the Anti-Wiretapping Law,[89] the Secrecy of Bank Deposits Act[90] and the Intellectual

---

87. REVISED PENAL CODE, arts. 290 to 292 provide:

> DISCOVERY AND REVELATION OF SECRETS
>
> Art. 290. Discovering secrets through seizure of correspondence. — The penalty of prision correccional in its minimum and medium periods and a fine not exceeding 500 pesos shall be imposed upon any private individual who in order to discover the secrets of another, shall seize his papers or letters and reveal the contents thereof.
>
> If the offender shall not reveal such secrets, the penalty shall be arresto mayor and a fine not exceeding 500 pesos.
>
> The provision shall not be applicable to parents, guardians, or persons entrusted with the custody of minors with respect to the papers or letters of the children or minors placed under their care or study, nor to spouses with respect to the papers or letters of either of them.
>
> Art. 291. Revealing secrets with abuse of office. — The penalty of arresto mayor and a fine not exceeding 500 pesos shall be imposed upon any manager, employee, or servant who, in such capacity, shall learn the secrets of his principal or master and shall reveal such secrets.
>
> Art. 292. Revelation of industrial secrets. — The penalty of prision correccional in its minimum and medium periods and a fine not exceeding 500 pesos shall be imposed upon the person in charge, employee or workman of any manufacturing or industrial establishment who, to the prejudice of the owner thereof, shall reveal the secrets of the industry of the latter.

88. REVISED PENAL CODE, art. 280 provides:

> Art. 280. Qualified trespass to dwelling. — Any private person who shall enter the dwelling of another against the latter's will shall be punished by arresto mayor and a fine not exceeding 1,000 pesos.
>
> If the offense be committed by means of violence or intimidation, the penalty shall be prision correccional in its medium and maximum periods and a fine not exceeding 1,000 pesos.
>
> The provisions of this article shall not be applicable to any person who shall enter another's dwelling for the purpose of preventing some serious harm to himself, the occupants of the dwelling or a third person, nor shall it be applicable to any person who shall enter a dwelling for the purpose of rendering some service to humanity or justice, nor to anyone who shall enter cafes, taverns, inn and other public houses, while the same are open.

Property Code[91] also penalize an unauthorized intrusion into the privacy of an individual. The Rule on Evidence regarding privileged communication was also seen in *Ople* as a recognition the privacy of certain information.[92]

However, the right to privacy is not absolute. As noted in *Ople*, "intrusions into the right must be accompanied by proper safeguards and well-defined standards to prevent unconstitutional invasions... [A]ny law or order that invades individual privacy will be subjected by this Court to strict scrutiny."[93]

B. Arguments in favor of a National ID System

The benefits derived from the creation of massive personal data systems based on a large number of people, also known as mass *dataveillance*,[94] have been raised as late as 1988 in a paper by computer scientist Roger Clarke, who claims that "[s]ignificant benefits can result from dataveillance. The physical security of people and property may be protected, and financial benefits may accrue from the detection and prevention of various forms of error, abuse, and fraud."[95]

Information Technology Law and United States Constitutional Law writer A. Michael Froomkin of the University of Miami notes that there are four areas in general which stand to benefit with regard to information gathering linked to a national identification system:

1. Information on personal biometric data;
2. Information on past activities;

---

89. An Act to Prohibit and Penalize Wire Tapping and other Related Violations of the Privacy of Communication, and for other Purposes, Republic Act No. 4200 (1965).

90. An Act Prohibiting Disclosure of or Inquiry into, Deposits with any Banking Institution and Providing Penalty Therefor, Republic Act No. 1405 (1955).

91. An Act Prescribing the Intellectual Property Code and Establishing the Intellectual Property Office, Providing for its Powers and Functions, and for other Purposes, Republic Act No. 8293 (1997).

92. REVISED RULES ON EVIDENCE, Rule 130 [C], §24.

93. Ople v. Torres, 293 SCRA 141,169 (1998).

94. ROGER CLARKE, INFORMATION TECHNOLOGY AND DATAVEILLANCE, 31 Commun. ACM 498-51 (Nov. 1987) [hereinafter CLARKE, INFORMATION TECHNOLOGY]. (Roger Clarke defines dataveillance as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons.").

95. *Id.*

3. Information on present acts and activities; and

4. Information on future acts or activities.[96]

Froomkin holds that information on personal biometric data, if shared across government agencies can be an effective tool against certain types of criminal offenders such as rapists, whose DNA, if so stored in a national database, could suggest the probability of the suspect's presence at the scene of a crime. Other permanent personal attributes could be better identified with a certain person such that when taken together creates very strong verification of a person's identity was also cited to have wide applications in the public sector, from social security to public health, and in the private sector as well, such as in banking.[97]

Information on one's past activities, in Froomkin's view, could relate to information regarding one's credit history, past employment, acquaintances, criminal records, and the like.[98] Information on present activities monitors actions that occur in real-time. The data collected from this infobase is beneficial to the government in terms of tax collection, where a closer eye can now be kept on the transactions of an individual, allowing the government to promptly collect on income improperly declared. Even if these gains were not to be realized, Froomkin notes that government may still benefit from the data in terms of economic development, as a measure of economic progress.[99] This link to economic development is highlighted in E.O. 420 as it delegates to the National Economic Development Authority the power to coordinate the development of the national identification system.[100]

In his paper,[101] Clarke lists several benefits that may accrue to mass dataveillance, among which is, increased government efficiency, and is thus reflected in E.O. 408. This increased efficiency may be directly attributed also to the increased efficiency brought about by the sharing of the aforementioned databases on biometrics, past, and present activities.

As noted in the Whereas Clauses of E.O. 408, there is a large amount of data redundancy in government.[102] In practice, many forms of identification

96. A. Michael Froomkin, The Uneasy Case for National ID Cards, *at* http://personal.law.miami.edu/~froomkin/articles/ID1.pdf (last accessed May 17, 2006).

97. *Id.* at 7.

98. *Id.* at 10.

99. *Id.* at 13.

100. E.O. 420, §4.

101. CLARKE, *supra* note 94.

102. E.O. 408, Whereas Clause.

are required to facilitate both public and private transactions, as many cards issued by different government agencies operate as *de facto* identity cards. It has been argued that the implementation of a national identification system would streamline government processes by reducing the number of levels one has to go through to verify one's identity. These integrated data systems can also go a long way in preventing fraud by providing more secure and transparent methods of sharing data.[103]

Froomkin notes in his paper on the subject that these large infobases can prove to be quite efficient, as such:

> If linked to extensive databases, biometric information, and real-time (or near-real-time) activity monitoring – all of which are possible, even likely, developments in the next decade – an ID card system can form the anchor of a wide-ranging system of surveillance, authorization and, optionally, control.[104]

Benefits accruing toward more effective national security must also not be overlooked, especially those resulting from information towards future acts or activities. Also, there is arguably a faster and more efficient method of authenticating raw data coming from the field. There is thus a greater capacity for control on the part of the government on its citizens as a direct result of such a system. Supporters of national identification systems argue that this intrusion into privacy is supported by citizens who have since grown weary from terrorism who are now willing to pay any price for the preservation of freedom, or what remains of such.[105]

C. Arguments against a National ID System

The main argument against the institution of a national ID system revolve around the right to privacy as guaranteed in the Bill of Rights.

Clarke's list of the dangers of mass dataveillance with respect to an individual are also regarded by Froomkin as canon in his paper on a national ID system for the United States:

1. Witch hunts;
2. Ex-ante discrimination and guilt prediction;
3. Selective advertising;
4. Inversion of the onus of proof;

---

103. CLARKE, *supra* note 94.

104. *The Uneasy Case for National ID Cards*, *supra* note 96, at 4.

105. British National Identity Card, *supra* note 49. *See also* Australian Privacy Foundation *at* http://www.privacy.org.au/Campaigns/ID_cards/NatIDScheme.html (last accessed May 16, 2006).

5. Covert operations;

6. Unknown accusations and accusers; and

7. Denial of due process.

Witch hunts are possible because mass dataveillance allows police to isolate, identify, and harass certain people matching a certain perceived characteristic without any indication of wrongdoing on the part of the person. From the same causes arise ex-ante discrimination and guilt prediction, which eventually lead to a denial of due process. Clarke explains the problem thus:

> Statistical techniques such as multivariate correlation and discriminant analysis have limited domains of applicability that are often poorly understood or ignored. Even if the statistical procedures are properly applied, a profile needs to be justified by systemic reasoning. In the hands of the inadequately trained, insufficiently professional, or excessively enthusiastic or pressured, profiling has all the hallmarks of a modern witch-hunting tool.

Froomkin also enumerates five risks associated with national identification systems, which may come from both public and private actors: risks from the legal use of accurate information, risks from illegal use of accurate information; risk of reliance on false information; risk of intentional creation of false information; risk of over-dependance on some feature of the system (completeness of database, ubiquity of card or other token).[106] Froomkin points out that even though the use of the identification system may be legal, this is no guarantee that there are no privacy issues raised nor any harm done. He raises the specter of danger from data mining; anonymous denunciations; class profiling; and efficient stigmatization – all from the legal use of the gathered data. He also warns of the moral and psychological costs of such an identification system.[107]

Such data mining would allow government to go on so-called "fishing expeditions" currently banned by the exclusionary rule and the principle of due process.[108] Predictive profiling, a direct result of such data mining has been proven to create false positives that are, although easy to introduce into the system, hard to remove.[109] In the United States, registered sex offenders

---

106. *The Uneasy Case for National ID Cards*, *supra* note 96, at 27.

107. *Id.* at 44.

108. *Id.*

109. *Id.* (Froomkin cites the case of Richard Jewell as a prime example of a false positive resulting from predictive profiling.). *See generally* Richard Jewell v. NBC, and Other Richard Jewell cases, *at* http://medialibel.org/cases-conflicts/tv/jewell.html (last accessed May 16, 2006).

have reported discrimination as a result of Megan's law, which mandates states to identify their current residences to communities even after they have been reintegrated into society.[110] Finally, Froomkin notes that there is a moral and psychological value to a citizen living a virtuous life without having to resort to artificial means to establish his or her identity.

Perhaps the best words arguing against the institution of mass dataveillance systems come from Clarke's last words in his enumeration of the benefits of dataveillance:

> ...[D]ataveillance is, by its very nature, intrusive and threatening. It therefore seems reasonable that organizations should have to justify its use, rather than merely assuming its appropriateness.

VII. CASE LAW

Due to the technology inherent in creating such a large, coherent database to warrant a judicial inquiry on the right to privacy, jurists consistently cite two cases that deal quite exhaustively on the matter, as far as the present issue is concerned: *Whalen v. Roe*,[111] a 1972 case that deals with the creation of a health prescription database in the New York area; and *Ople v. Torres*, a decision by the Philippine Supreme Court that touched on the issue of the right to privacy. *Whalen* was recognized in the present case as the definitive standard set by the United States Supreme Court by which government may collect data from its citizens.

A. Whalen v. Roe

The New York Legislature in 1972 enacted a statute which classified potentially harmful drugs and provided that prescriptions for the category Schedule II embracing the most dangerous legitimate drugs be prepared on an official form, a copy of the form, which requires identification of the prescribing physician, dispensing pharmacy, drug and dosage, and the patient's name, address, and age, must be filed with the State Health Department, where pertinent data are recorded on tapes for computer processing.[112] All forms are required to be retained for a five-year period under a system to safeguard their security, and are thereafter destroyed. Public disclosure of the patient's identity is prohibited, and access to the files is confined to a limited number of health department and investigatory personnel.[113]

---

110. *Id.*

111. Whalen v. Roe, 429 U.S. 589 (1977).

112. *Id.*

113. *Id.*

Roe brought an action challenging the constitutionality of the Schedule II patient-identification requirements. Holding that "the doctor-patient relationship is one of the zones of privacy accorded constitutional protection" and that the Act's patient-identification provisions invaded that zone with "a needlessly broad sweep," since the Commissioner of Health of New York, Whalen, had been unable to demonstrate the need for those requirements, a three-judge District Court enjoined the enforcement of the challenged provisions.[114]

In this case, the Court recognized the "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks..." and observed that "The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures."[115]

B. Ople v. Torres

This is the most controversial so far on the issue that discusses the merits for and against the implementation of a national ID system.

In this case, the late Senator Blas F. Ople assailed the validity of Administrative Order No. 308 on two important constitutional grounds. One, it is a usurpation of the power of Congress to legislate, and two, it impermissibly intrudes on our citizenry's protected zone of privacy. Although the Court recognized that the President had administrative power to apply policies, enforce orders, and to fix a uniform standard of administrative efficiency and to check the official conduct of his agents through the issuance of administrative orders, rules and regulations,[116] it held that Administrative Order No. 308 involves a subject that is not appropriate to be covered by the President's administrative order. Section 3, Chapter 2, Title I, Book III, Administrative Code of 1987 defines administrative orders as, "[a]cts of the President which relate to particular aspects of governmental operation in pursuance of his duties as administrative head," and as such "it must be in harmony with the law and should be for the sole purpose of implementing the law and carrying out the legislative policy."[117]

As to the issue on privacy, the Court held that Administrative Order No. 308 cannot pass constitutional muster as an administrative legislation

---

114. *Id.*

115. *See* Eleanor Eisenberg, Comments of the Arizona Civil Liberties Union, Privacy Considerations and Public Access to Electronic Court Records, *at* http://www.courtaccess.org/legalwritings/eisenberg2000.doc (last accessed May 15, 2006).

116. VINCENT G. SINCO, PHILIPPINE POLITICAL LAW 234-35 (1962).

117. IRENE R. CORTES, PHILIPPINE ADMINISTRATIVE LAW, 2-5 (1984).

because facially, it violates the right to privacy. The Court explained that the said order, "falls short of assuring that personal information which will be gathered...will only be processed for unequivocally specified purposes." Furthermore, the lack of proper safeguards and the possibilities of abuse and misuse of the information threaten the very abuses that the provisions on privacy enshrined Bill of Rights seek to prevent.

VIII. A CRITIQUE OF E.O. 420

Does E.O. 420 establish a National ID System?

It is the argument of the Supreme Court that E.O. 420 does not establish a National ID System but merely "makes the existing sectoral card systems of government entities like GSIS, SSS, Philhealth and LTO less costly, more efficient, reliable and user-friendly to the public."[118]

E.O. 420 does not compel all citizens to have an ID card and applies only to government entities that under existing laws are already collecting data and issuing ID cards as part of their governmental functions. The Court rationalized that "a national ID card system requires legislation because it would necessarily create 'a new national data collection and card issuance system.'"[119] As such, it concluded that no new system was contemplated in the executive order when it held that:

> *Every government entity that presently issues an ID card will still issue its own ID card under its own name.* The only difference is that the ID card will contain only the five data specified in Section 3 of EO 420, plus the fingerprint, the agency ID number, and the common reference number which is needed for cross-verification to ensure integrity and reliability of identification.

However, it is the author's opinion that E.O. 420 does establish such a new data collection and card system. This intention is belied in the second whereas clause of the new executive order:

> *WHEREAS*, the existing *multiple identification systems in government have created unnecessary and costly redundancies* and higher costs to government, while making it *inconvenient for individuals to be holding several identification cards*;[120]

The issuance of the same identification cards, but with common data, as envisioned by the Supreme Court is anathema to this whereas clause, which

---

118. Kilusang Mayo Uno, et al., v. the Director-General, et al., G.R. No. 167798, April 19, 2006.

119. *Id.*

120. E.O. 420, Whereas Clause (emphasis supplied).

specifically mentions the cost involved in the issuance of several identification cards.

This intention is also belied by the standards set in Section 6 of E.O. 420 itself, which provides:

> Section 6. *Safeguards*. – The Director-General, National Economic and Development Authority, and the pertinent agencies shall adopt such safeguard as may be necessary and adequate to ensure that the right to privacy of an individual takes precedence over efficient public service delivery. Such safeguards shall, as a minimum, include the following:
>
> a. The data to be recorded and stored, which shall be *used only for purposes of establishing the identity of a person*, shall be limited to those specified in Section 3 of this executive order;[121]
>
> xxx xxx xxx

It is of note that nothing in the executive order supports the conclusion of the High Court that the existing government agencies and government-owned and controlled corporations already issuing identification cards are to continue issuing their identification cards, and that all that E.O. 420 refers to is a shared identification database.

Even if the whereas clause would be construed to refer to a shared information database, do existing systems not already provide the same purpose? Birth certificates, as printed on National Statistics Office security paper are presently used to establish one's identity across all branches of government. So too, are driver's licenses and passports, for that purpose.

It is the burden of the government to show that the statute allegedly infringing on a right is narrowly drawn and constitutional.[122] Thus, this author poses that there is an inconsistency between this decision and the one reached in Ople. Perhaps the insight of Justice Puno was missed in the discussion therein.[123]

IX. E.O. 420 AND THE RIGHT TO PRIVACY

The main contention of those critical to Executive Order No. 420 is that it disregards the conclusions set in *Ople*. At first glance, the present case regarding the constitutionality of E.O. 420 seems to be no different from the case of Administrative Order No. 308. Both are issuances from the executive

---

121. E.O. 420, § 6.

122. Ople v. Torres, 293 SCRA 141, 166 (1998).

123. Justice Puno was not present during the deliberations as he attended to the wake of his late wife, the former Supreme Court Clerk of Court Luzviminda Puno.

branch that seek the establishment of an integrated identification system. Both orders have the same goal of enhancing the efficiency of government and governmental transactions. A.O. 308 sought to provide "Filipino citizens and foreign residents with the facility to conveniently transact business with basic service and social security providers and other government instrumentalities" through a "computerized system to properly and efficiently identify persons seeking basic services on social security and to reduce… fraudulent transactions and misrepresentations."

Likewise, E.O. 420 recognized the "urgent need to streamline and integrate the processes… in government to reduce costs and to provide greater convenience for those transacting business" and to "facilitate private businesses, enhance the integrity and reliability of government-issued identification cards in private transactions, and prevent violations of laws involving false names and identities."

In *Ople*, the Court took a proactive stand, declaring that "the indefiniteness of A.O. 308 can give the government the roving authority to store and retrieve information for a purpose other than the identification of the individual through his PRN."[124] The Court said that:

> The potential for misuse of the data to be gathered under A.O. 308 cannot be underplayed as the dissenters do. Pursuant to said administrative order, an individual must present his PRN everytime he deals with a government agency to avail of basic services and security. His transactions with the government agency will necessarily be recorded – whether it be in the computer or in the documentary file of the agency. The individual's file may include his transactions for loan availments, income tax returns, statement of assets and liabilities, reimbursements for medication, hospitalization, etc. The more frequent the use of the PRN, the better the chance of building a huge and formidable information base through the electronic linkage of the files. The data may be gathered for gainful and useful government purposes; but the existence of this vast reservoir of personal information constitutes a covert invitation to misuse, a temptation that may be too great for some of our authorities to resist.[125]

The Solicitor General also stated that the adoption of the Identification Reference System will contribute to the "generation of population data for development planning," which to the Supreme Court is an admission that the PRN will not be used solely for identification but for the generation of other data with remote relation to the avowed purposes of A.O. 308."[126]

---

124. *Ople*, 293 SCRA at 161.

125. *Id.*

126. *Id.* at 160.

It is clear from the foregoing argument of the ponencia that A.O. 308 threatened the right to privacy by not specifying what particular biometric data and technology will be used in the integrated identification system. In the words of the Supreme Court:

> A.O. 308 does not state what specific biological characteristics and what particular biometrics technology shall be used to identify people who will seek its coverage. Considering the banquet of options available to the implementors of A.O. 308, the fear that it threatens the right to privacy of our people is not groundless.

The Supreme Court in *Ople* further laid down the additional standard that the government must specifically state for what purpose information gathered should be used. Without a limitation as to the purpose for which such gathered data is to be used, the intrusion must be declared unconstitutional.

> [A.O. 308] does not provide who shall control and access the data, under what circumstances and for what purpose. These factors are essential to safeguard the privacy and guaranty the integrity of the information. Well to note, the computer linkage gives other government agencies access to the information. Yet, there are no controls to guard against leakage of information. When the access code of the control programs of the particular computer system is broken, an intruder, without fear of sanction or penalty, can make use of the data for whatever purpose, or worse, manipulate the data stored within the system. [127]

There lies the difference between the case of *Ople* and that of the present case in *Kilusang Mayo Uno v. the Director General.* The Supreme Court found that E.O. 420 specificially defines which data is to be collected and used among all government agencies, *viz*:

> Section 3 of E.O. 420 limits the data to be collected and recorded under the uniform ID system to only 14 specific items, namely: (1) Name; (2) Home Address; (3) Sex; (4) Picture; (5) Signature; (6) Date of Birth; (7) Place of Birth; (8) Marital Status; (9) Name of Parents; (10) Height; (11) Weight; (12) Two index fingers and two thumbmarks; (13) Any prominent distinguishing features like moles or others; and (14) Tax Identification Number.[128]

The ID card itself under E.O. 420, while limited to the fourteen specific items above, is to show only eight specific data. Under Section 3 of E.O. 420,

---

127. *Id.* at 162.

128. Kilusang Mayo Uno, et al., v. the Director-General, et al., G.R. No. 167798, April 19, 2006.

> [A] corresponding ID number will be issued by the participating agency and a common reference number shall form part of the stored ID data and, together with at least the first five items listed above, including the print of the right thumbmark, or any of the fingerprints as collected and stored, shall appear on the face or back of the ID card for visual verification purposes.[129]

The limitation of the collected data itself does not make E.O. 420, *per se* valid but the kind of information collected under the E.O. 420 is what makes the order more palatable. The data collected under E.O. 420 is data that already forms part of existing government ID cards. Unlike A.O. 308, E.O. 420 does not establish an overbroad and vague integrated identification system that does not specify what kind of information is to be collected but makes use of information that is already being used.

Unlike A.O. 308, E.O. 420 prescribes safeguards on the collection, recording, and disclosure of personal identification data to protect the right to privacy.[130]

While A.O. 308 forgets to specify any safeguards with regard to changes and revisions in the data collected, E.O. 420 provides that the information collected and stored shall be kept and treated as strictly confidential and the owner's written personal or written authorization is required for the access, disclosure of data, revision or corrections to the information.

Although E.O. 420 still does not provide for specific guidelines about data control, a general indication of "stringent systems of access control to data" is obviously better than a system that fails to mention any kind of data control.

However, privacy issues with regard to the use of the integrated data were not fully addressed by the Court in the present case.

The use of the integrated ID for purposes of identification cannot truly be said to be limited to government agencies and functionaries. The convenience created by the existence of the card ensures that in the future, such card will extend not only to all governmental functions or agencies but also to commercial transactions. This process is known as *functionality creep*, and has been defined as "what occurs when an item, process, or procedure designed for a specific purpose ends up serving another purpose for which it was not intended."[131]

---

129. E.O. 420, § 3.

130. E.O. 420, § 6.

131. Wikipedia. Functionality Creep, *at* http://en.wikipedia.org/wiki/Functionality_creep, (last accessed May 16, 2006).

The Anti-Money Laundering Act of 2001 provides a good case in point. Section 9 of the Anti-Money Laundering Act provides the necessary standards for customer identification.

> *SEC. 9. Prevention of Money Laundering; Customer Identification Requirements and Record Keeping.* - (a) *Customer Identification.* - Covered institutions *shall establish and record the true identity of its clients based on official documents.* They shall maintain a system of verifying the true identity of their clients and, in case of corporate clients, require a system of verifying their legal existence and organizational structure, as well as the authority and identification of all persons purporting to act on their behalf.
>
> The provisions of existing laws to the contrary notwithstanding, anonymous accounts, accounts under fictitious names, and all other similar accounts shall be absolutely prohibited. Peso and foreign currency non-checking numbered accounts shall be allowed. The BSP may conduct annual testing solely limited to the determination of the existence and true identity of the owners of such accounts. [132]

It is not a stretch to see that at some point, the official documents referred to by said Act could refer to just that single card comprehended under E.O. 420, if only for convenience and for efficiency of the banking sector. Therefore, inasmuch as it creates a convenient, single system for identity verification, the arguments as to the private use of such a system must be addressed, as the functions to which it will be applied creates indirect pressure on the ordinary citizen to acquire one.[133]

The net effect of the integrated government ID envisioned by E.O. 420 is to create a standard identification system for all governmental transactions. These protections seem to be more illusory than real at this stage, as these transactions are dependent on the accurate input of data into the system, and no safeguards are explicitly set forth to ensure that no false data is entered.[134]

As expressed earlier, concerns about the capacity for misuse of the system are not satisfied by an express declaration that the data is to be used for identity verification only, as the characteristics found that describe one person are sufficient to create a whole range of public and private applications.[135]

The argument comparing the data compiled in the unified government ID created by E.O. 420 to the Supreme Court employees' ID, to the author is inaccurate. The Supreme Court employee ID card does not restrict or

---

132. An Act Defining the Crime Of Money Laundering, Providing Penalties Therefor and for other Purposes, Republic Act 9160 (2001) (emphasis supplied).

133. *National Identification System: Do We Need One?, supra* note 4, at 4.

134. E.O. 420, § 6.

135. *Id.*

regulate access to the courts in much the same way that existing identification systems restrict or regulate access to certain services or privileges, such as passports or driver's licenses do. As such, the employee ID card used by the Supreme Court is not as vulnerable to the functionality creep danger that lurks in the creation of a national identification system.

Finally, the Supreme Court skipped the concerns of individuals in placing so much information regulating access to governmental functions in the hands of the executive, by declaring the discussion on privacy as *obiter dicta.*

> *Ople v. Torres* is not authority to hold that EO 420 violates the right to privacy because in that case the assailed executive issuance, broadly drawn and devoid of safeguards, was annulled solely on the ground that the subject matter required legislation. As then Associate Justice, now Chief Justice Artemio V. Panganiban noted in his concurring opinion in *Ople v. Torres*, "*The voting is decisive only on the need for appropriate legislation, and it is only on this ground that the petition is granted by this Court.*"[136]

X. CONCLUSION

The text of E.O. 420 is not clear on whether it establishes a new ID system or merely an integrated database. The Supreme Court, declaring the said executive order constitutionally sound, interpreted it to mean the latter, emphatically making a pronouncement that E.O. 420 does not establish a National ID System.

Seeing the decision in this light, the Court's pronouncement in the present case may be seen as complementary and not entirely antithetical to the decision in *Ople.* As the Court interpreted the executive order as merely an instruction to the National Economic Development Authority (NEDA) to create an extensive, shared infobase, and nothing more, it logically follows that *Ople* cannot be used as authority to hold that E.O. 420 violates the right to privacy.

The Supreme Court then looked at the standards set by *Whalen* in examining whether E.O. 420's intrusions on the right to privacy are justified. *Whalen* recognized that there is a "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files,"[137] and this "right to collect and

136. Kilusang Mayo Uno, et al., v. the Director-General, et al., G.R. No. 167798, April 19, 2006.

137. Whalen v. Roe, 429 U.S. 589 (1977).

use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures."[138]

In the words of Justice Brennan, a state's "collection and storage of data... that is, in itself, legitimate is not rendered unconstitutional simply because new technology makes the [s]tate's operations more efficient. However,... the Constitution puts limits not only on the type of information the state may gather, but also on the means it may use to gather it." A carefully designed program that includes numerous safeguards intended to forestall the danger of indiscriminate disclosure" and is successful in its efforts to "prevent abuse and limit access to the personal information" cannot amount to a "deprivation of constitutionally protected privacy interests, any more than the more traditional reporting provisions..."[139]

Our Supreme Court adopted these standards set by *Whalen* and ruled that the intrusions into the right of privacy by E.O. 420 is justified by compelling state interest and that it is narrowly drawn while prescribing comprehensive safeguards. However, our High Court loosely interpreted these safeguards to mean just a limitation on the kind of data gathered and blindly takes the government's word that this information will be restrictively used.

Restated, it seems that the Supreme Court is saying that, as long as there are safeguards indicated in the order, whether or not these safeguards are in reality adequate, the right to privacy on ordinary citizens cannot be said to be infringed.

However, the second whereas clause of E.O. 420 itself makes a declaration that "*existing multiple identification systems in government have created unnecessary and costly redundancies* and higher costs to government, while making it *inconvenient for individuals to be holding several identification cards.*"[140] This, to the author's mind is indicative of the intention of the government to establish just one integrated identification system and not just a shared information database. It would seem impractical, if not obtuse of the government to tout the benefits of having an "integrated ID card" and yet let different government agencies issue several different cards essentially having the same information and being issued for essentially the same purpose.

The issuance of several different identification cards, but with common data, as envisioned by the Supreme Court, is anathema to this whereas

138. *Id.*

139. *Id.* at 78.

140. E.O. 420, Whereas Clause (emphasis supplied).

clause, which specifically mentions the cost involved in the issuance of several identification cards.

The presumption made by the Supreme Court that E.O. 420 does not establish a sort of "National ID" because E.O. 420 puts a restriction *as to the kind of data to be collected and its use* seems to be an attempt to justify the constitutionality of the Executive Order in not so many words.

While it is true that E.O. 420 is not as constitutionally defective as its predecessor, A.O. 308, there are still privacy concerns that must be addressed. It does not follow that just because the system is to use data already required by specific government agencies, there is no national identification system created devoid of all hazards to the right to privacy. The mere deletion of the words "new" and "national" to qualify the word "identification" does not mean no new legal animal is created.

After all, it is a legal maxim that what governs is not the letter of the law but its spirit.