Penn State International Law Review

Volume 20
Number 2 *Penn State International Law Review*

Article 7

1-1-2002

Europe's Mobile Opportunity: Can the European Union Legislate Consumer Trust and Compete in the E-Commerce Market with the United States

Alfred Viloch III

Europe's Mobile Opportunity: Can the European Union Legislate Consumer Trust and Compete in the E-Commerce Market with the United States?

I. Introduction

Imagine that you're preparing for work in the morning. Before you walk out the front door, you remember to grab your mobile phone. As you look, you remember that it had been beeping all night. You find the phone and it displays, "50 new messages." The messages read, "Lose weight fast. Try Metabolean. Only $49." As you check the remaining messages, you realize they're the same as the first.[1] This example illustrates the significance of privacy legislation in the mobile wireless sector. If a phone beeps incessantly, the user will begin to ignore most of the beeps.[2] This annoyance might drive the user to ignore her mobile phone.[3]

Next, on your drive to work, you decide to transfer funds from your savings account to your checking account. You pick up your Internet-enabled mobile phone and make a request to your bank's web site. The web site asks for your account number, Social Security number, and a five-digit pin number. The funds are transferred smoothly; however, after two weeks, your bank statement shows that your funds have been removed without your knowledge. The bank suggests that you contact your service provider since no security breaches have occurred on its premises. When you reach your service provider, they mention that problems have occurred with their computers. An unauthorized person gained access to their wireless transmission computers and may

1. *See* Marcia Savage & Amanda Stirpe, *Under Surveillance: Location-Based Wireless Technology Raises Privacy Concerns for Solution Providers*, COMPUTER RESELLER NEWS, Dec. 4, 2000; *Cf.* Brian Fonseca, *Wireless Security Concerns*, INFOWORLD DAILY NEWS, June 8, 2000 (This hypothetical situation was based on the idea of unsolicited text messages).

2. *See* Savage & Stirpe, *supra* note 1.

3. *See id.*

have misused some information. This example illustrates the significance of security legislation in the mobile wireless sector.

Although the above hypothetical examples may seem infrequent, as the wireless Internet grows, so might these occurrences.[4] In an effort to address these privacy and security concerns, the European Union has proposed data protection directives that intend to harmonize the Member States' national laws in the electronic communications sector.[5] Consumer trust and confidence are critical factors in determining whether consumers will engage in wireless e-commerce.[6] The European Union intends to use data protection legislation as a tool to stimulate Europe's lagging Internet economy.[7]

Europe seeks to stimulate its e-commerce participation by taking advantage of new wireless Internet technologies.[8] Through Internet-enabled mobile phones, European citizens may have the ability to diminish the United States' e-commerce lead.[9] The U.S. has typically held a sizeable lead over Europe in this respect because Internet access has been traditionally limited to desktop computers: computers that are not as readily available to Europeans in their home countries. But, as Internet access becomes available through small wireless devices, Europeans will have the potential to join their American counterparts in the global e-commerce landscape.

The purpose of this comment is to suggest how the European Commission can update its data protection proposal to provide the privacy and security measures that are essential to promote e-commerce transactions. The timely passage of this legislation is critical for the European Union in order to stimulate its e-commerce. It has been suggested that Europe has a three-year

4. Fonseca, *supra* note 1. Wireless devices are expected to used as much as desktop computers in the next upcoming years.

5. Commission of the European Communities Proposal for a Directive of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, COM(00)385 final [hereinafter the Proposed Directive on Electronic Data Protection].

6. Robert J. Guttman, *Erkki Liikanen: European Commissioner for Enterprise and the Information Society*, EUROPE, May 2000, at 11.

7. *Id.*

8. Bruce Barnard, *Europe's Mobile Advantage*, EUROPE, May 2000, at 16. Europe maintains leadership in the mobile communications sector because of three factors: its early deregulation of its telecommunications markets, its single cross-border standard, its Member States' less stringent free speech requirements.

9. *Id.* Currently, the United States comprises of eighty percent of the global e-commerce market, while Europe comprises ten percent of this market. *Id.*

window of opportunity to catch the United States' level of e-commerce participation.[10] With this time constraint in mind, Europe must focus on two objectives in order to effectuate its goal of encouraging greater e-commerce participation among its citizens: First, it must update and adopt its Electronic Data Protection Proposal. Second, it must ensure that its Member States transpose this legislation in a timely manner.

This comment is divided into five sections. After this introduction, Part II will explore the recent developments in wireless Internet access and wireless e-commerce. At this point, in its early development, the wireless Internet suffers from growing pains.[11] It is at its infancy, and this technology is raising similar privacy and security concerns as the wired Internet did years ago.[12] Generally, these concerns are focused on the privacy and security of personal information.[13] If the European Union intends to take advantage of recent wireless developments, then effective data protection legislation is imperative to promote e-commerce growth.[14] Consumers will be wary of privacy issues and this apprehension will affect their mobile phone use.[15]

Security concerns lead us to Part III, which will analyze the European Union's current data protection legislation. The European Union has embodied this legislation in Directives 95/46[16] and 97/66,[17] which were created to harmonize the Member States'

10. Guttman, *supra* note 6, at 11.

11. John Yaukey, *Dial I for Internet: Wireless Application Protocol Brings Access to Your Cell Phone*, THE SALT LAKE TRIB., Feb. 26, 2000, at D10. These growing pains are associated with lack of privacy and security measures.

12. *Id.*

13. *See generally* Kelly Carroll, *Partnering for a Secure Market*, TELEPHONY, Jan. 10, 2000, at 40; *see generally*, Keith Perine, *Talking About Wireless Privacy*, THE INDUSTRY STANDARD, Dec. 25, 2000. Personal information may include: location information, government-issued identification numbers, credit card or similar financial information, and health-related information.

14. Guttman, *supra* note 6, at 11 (A clear and concise legislative framework is vital to ensure consumer trust).

15. Axel Krause, *Interview with David Aaron*, EUROPE, May 2000, at 16 (explaining that the Internet, as booming as it is in the United States, would be 30 to 40 percent more robust with regard to commercial use if [American consumers] felt it were more secure).

16. European Parliament and Council Directive 95/46 of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) [hereinafter the Data Protection Directive].

17. European Parliament and Council Directive 97/66 of 15 December 1998 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 1998 O.J. (L024) [hereinafter the Telecommunications Directive].

national laws[18] and to ensure the fundamental right of privacy.[19] However, as this section will suggest, this legislation has flaws. For the most part, its language is technology-specific and does not contemplate recent wireless developments.[20] Rather, these directives focus on voice telephony and will fail to protect users of Internet-enabled mobile phones.[21] Also, these directives fail to contemplate privacy issues concerning location technology.[22] These limitations and oversights have prompted the European Commission to draft legislative proposals to address these concerns.

Part IV will discuss this proposed legislation. The Commission has drafted these proposals to address two major areas of concern: the employment of technology-neutral language for broader applications to future technologies, and the issues associated with the collection and use of location data.[23]

Parts V and VI will examine the Member States' implementation of current data protection legislation and will explain how timely legislation is an important factor in gaining consumer trust. Specifically, some Member States have failed to implement the EU's current data protection legislation[24] while other states have gradually implemented these directives. This section suggests that implementation problems by some States may impede the timeliness of Europe's e-commerce advance, thereby defeating Europe's ability compete at the U.S.'s level. As discussed earlier, Europe's e-commissioner believes that if Europe does not catch the United States' Internet economy within three years, the United States' lead will become insurmountable.[25]

---

18. Data Protection Directive, *supra* note 16, at 32. Some countries did not have any data protection privacy as of the data of this directive.

19. *Id.* at 31.

20. Commission of the European Communities Proposal for a Directive of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, COM(00)385 final. The Telecommunications Directive's terminology focuses on voice telephony and will not properly harmonize laws concerning electronic communications, i.e., Internet communications and text messages.

21. *Id.* at 2.

22. *Id.* at 3. Location data is defined as being data which reveals the users location, or technically, the location of the user's handset.

23. *Id.* at 2-3. A problem associated with location data is constant unauthorized surveillance of the mobile phone user.

24. Data Protection: Implementation of 95/46, *at* http://europa.eu.int/comm/nternal_market/en/media/dataprot/law/impl.htm (last visited Jan. 18, 2001) (as of Jan. 18, 2001, five Member States have failed to implement the European Union's data protection legislation).

25. Bruce Barnard, *Is Europe Ready for the E-Future*, EUROPE, May 2000, at 8.

Finally, Part VII suggests how the European Union, through legislation, can help its Member States stimulate its e-commerce economy. With the doctrine of "direct effect," the European Union has the power to create a directive that will protect consumers regardless of the Member States' lagging implementation measures. With the help of this provision, the European Union can legislate timely data protection laws that will provide consumer comfort in this new and innovating area of commerce.

II. Wireless Internet Technologies

The purpose of this section is to review the developments in mobile wireless Internet technologies and to present a general overview of the privacy and security issues associated with this technology. This section, however, will begin by discussing Europe's leadership in mobile communications and the reasons why the United States lags behind.

A. Europe's Mobile Advantage

Traditionally, the United States has been recognized as an e-commerce and Internet juggernaut.[26] Its e-commerce participation is mainly attributable to its citizens' access to desktop computers.[27] Other countries with less access to desktop computers, like the European countries, have lagged behind the United States with no hope of rising to the U.S.'s level of participation.[28] Some commentators believe that these countries will take several years to catch the United States' current technology. In fact, the United States' dominance in the desktop-computer arena is overwhelming. For instance, the United States accounts for nearly eighty percent of global e-commerce, while European countries comprise only ten percent.[29] Despite this disparity, Europe, through a nontraditional medium, may challenge the United States' e-commerce supremacy.

Recent developments in mobile communications have given consumers the ability to access the Internet by using a mobile phone.[30] This technology is called the wireless Internet. Now,

---

26. *See id.*

27. Krause, *supra* note 15, at 17.

28. Victoria Shannon, *E-Commerce Engages Europe, Slowly*, INT'L HERALD TRIB., June 19, 2000 at 13; *see* Krause, *supra* note 15, at 17 (instead of waiting to become strong in a weak area, Europe will be able to adapt a strong area to become stronger in its weak area, namely telecommunications and e-commerce).

29. Barnard, *supra* note 8, at 16.

30. Wapforum.org, *What WAP is and WAP Forum?*, *at* http://www.wapforum.org/faqs/index.htm (last visited Jan. 18, 2001).

instead of using a costly desktop computer to access the Internet, consumers may use a cellular phone.[31] These Internet-ready phones are less expensive and more affordable than desktop computers. The mobile phone's affordable nature makes the Internet more readily available to consumers.[32] In addition to affordability, Europe is a world leader in mobile communications.[33] Its leadership in the mobile communications industry has lasted for three years, thereby positioning itself to become a world leader in mobile Internet and mobile e-commerce.[34] Thus, instead of lagging behind the United States for several years in Internet participation, Europe can capitalize on both its mobile advantage and recent mobile technologies to reconcile the above disparity.[35]

European leadership in the mobile communications sector is based on three factors. First, Europe has deregulated its national telecommunications markets.[36] This deregulation allows mobile service providers to enjoy legal and technological uniformity among the nations and provides consumers with competitive service pricing. Second, Europe, through the European Union, has established a single cross-border standard.[37] Again, this facilitates the development of digital technology by providing uniformity of standards among the European nations. Finally, free speech protection in the European countries is not as stringent as in the United States, which allows the European Union to regulate the flow of information more efficiently.

In January 1998, Europe deregulated its telecommunications markets and prices for telephone services began to tumble.[38] This deregulation resulted in telephone companies having to lower their prices to compete in the telecommunications market.[39] These lower prices included discounts to prevent customers from dropping their carrier and obtaining services from other carriers.[40] As a result of deregulation, consumers were able to obtain telephone services at affordable prices. With affordable services, Europe is now able to

31. Anonymous, *The Internet Unplugged*, FORTUNE, Jan. 1, 2001, at 160.
32. *See id.*
33. Shannon, *supra* note 28.
34. Guttman, *supra* note 6, at 11.
35. Barnard, *supra* note 25, at 8.
36. Barnard, *supra* note 8, at 15.
37. *Id.* (Europe deregulated its telecommunications market in January 1998).
38. Kristi Essick, *Ringing in European Changes*, INFOWORLD, Dec. 29, 1997, at 1, 43.
39. *Id.*
40. *Id.*

compete with the United States' telecommunications sector.[41] Because voice telephony has become more affordable, European consumers will likely have the ability to obtain mobile Internet access through these same telephone service providers.

Another reason Europe enjoys its mobile advantage over the United States is because the American government has failed to set a single wireless-transmission standard.[42] Instead, the United States has developed an "incompatible hodgepodge of towers, services, and phones."[43] These incompatible towers and services have resulted in the United States having to create multiple cellular standards. These multiple standards coupled with the less efficient analogue system makes it harder for manufacturers to adapt their phones for new technologies.[44] Manufacturers find it difficult to update the American telecommunications market to the newer technologies. As a result, the United States is usually left behind to its disadvantage.

Europe, on the other hand, has a single cross-border standard.[45] This single standard allows Europe to upgrade to the faster technologies for the wireless Internet.[46] Since the cellular phone industry creates technologies geared towards this single standard, Europe is in a better position than the United States to benefit from wireless Internet technologies.[47] While the United States must adapt their wireless devices to different platforms and towers, Europe adapts its phones only to a single form of towers. This single standard is the equivalent of conversing in a single adopted language, while numerous standards require phones to converse in several languages.

Finally, Europe is in a better position to take advantage of the wireless Internet since its countries' constitutions do not contain strict free speech requirements.[48] With the United States guarantee of free speech, the First Amendment imposes some limits on the government's ability to regulate the flow of information, specifically personal data.[49] "[T]he [U.S.] Constitution includes specific

41. *Id.*
42. Walt Mossberg, *Technology: Walt Does Wireless*, WALL ST.J., September 29, 2000, at W1.
43. *See id.*
44. Barnard, *supra* note 8, at 14.
45. *Id.* at 15.
46. Mossberg, *supra* note 42.
47. *Id.*
48. Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 471 (2000).
49. *Id.*

protections that may pose obstacles to the implementation of European-style privacy regulation."[50] While the United States is restricted by its constitution, European countries with less stringent constitutional protections, through the European Union, may legislate uniform guidelines on data protection and consumer privacy. Europe, by way of less stringent free speech requirements, has more flexibility in creating "overarching" privacy laws. Uniform laws give Europe an advantage over the United States since consumers can rely on equal amounts of protection.

While the United States' First Amendment vigorously protects freedom of speech, this protection also makes some preventative legislation difficult. As a result, the "patchwork" of American laws results in proactive rather than preventative legislation.[51] The United States creates legislation in response to issues rather than creating legislation that contemplates future issues.[52] As a result of uniform legislation, Europe exists in a favorable environment to stimulate its mobile wireless Internet participation.

Europe, however, still needs to address the wireless industry's privacy and security concerns. This comment will address two of these two concerns by discussing consumer trust and the slow implementation of data protection directives in the European Union.

If the European Union does not address the above concerns in the next three years, the United States will build an insurmountable lead in the Internet economy.[53] Therefore, the European Union must legislate consumer trust to compete in the e-commerce market with the United States.[54] If Europe provides adequate data protection directives, it may "leap-frog" the United States in e-commerce participation. This possibility is mainly attributable to the advent of the Wireless Application Protocol.[55]

B. Wireless Application Protocol

Wireless Application Protocol (WAP) is a new technological development that allows users of mobile phones to interact with information and services immediately.[56] With WAP, a mobile phone communicates with the Internet through the user's service

50. *Id.*
51. *Id.*
52. *Id.*
53. Barnard, *supra* note 25, at 8.
54. Guttman, *supra* note 6, at 13.
55. Shannon, *supra* note 28.
56. Greg R. Notess, *From the Web to WAP*, ECONTENT, Aug/Sep 2000, at 69.

provider and WAP is the language the phone uses.[57] WAP allows a consumer, using her mobile phone, to access the Internet through the phone's small screen.[58] Not only can this consumer access the Internet through her phone, but also she can be an active participant.[59] She can make purchases and reservations, or request directions by simply using the phone's buttons.[60] WAP will allow this consumer to engage in e-commerce without having to use a desktop computer.[61]

WAP provides the technology whereby a mobile phone user may access the Internet through his phone's screen.[62] With WAP, a user enters a request on her mobile phone to interact with a web site.[63] Relying on WAP, the user's phone transfers wirelessly this Internet request to a WAP gateway (or proxy server) on the service provider's premises.[64] The WAP gateway is a computer that receives, decrypts, and re-encrypts the WAP transmission to be sent to the requested web site.[65] In other words, the WAP gateway sends the information in an understandable language to the Internet web site. The web site responds with the requested information, and the WAP gateway decrypts and re-encrypts the information into a language understandable by the user's mobile phone. The WAP gateway is merely a translator.

The phone receives the communications from the WAP gateway, and the phone's screen acts as a mini-web browser.[66] The mini-web browser displays specially formatted web pages from the Internet.[67] If the contacted web site does not offer this special web page format, then the handset is unable to display this site.[68]

This new technology is a distinct advantage for European countries. Over forty percent of Europeans currently own a mobile

57. Steve Grossman, *Mini-Certificate Program for Wireless Servers and Gateways*, ELEC. DESIGN, May 29, 2000, at 36.

58. Jason Levitt, *Wireless Devices Present New Security Challenges—Growth in Wireless Internet Access Means Handhelds will be Targets of More Attacks*, INFORMATIONWEEK, Oct. 23, 2000.

59. Wap Forum, *Why Go for WAP?*, *at* http://www.wapforum.org/faqs/index_new.htm#faq03 (last visited Jan 18, 2001).

60. *Id.*

61. *See* Anonymous, *supra* note 31.

62. Wap Forum, *supra* note 59.

63. Mossberg, *supra* note 42, at W.1.

64. Grossman, *supra* note 57, at 36.

65. Matt Hamblen, *Wireless Insecurity*, COMPUTERWORLD, Sep. 4, 2000, at 72.

66. Wap Forum, *Why Go for Wap?*, at http://www.wapforum.org/faqs/index_new.htm#faq03 (last visited Jan. 18, 2001).

67. Levitt, *supra* note 58.

68. *Id.*

phone in comparison to only twenty-five percent of Americans, and half of those Americans are still using the less efficient analogue system.[69] By 2003, approximately sixty-six percent of Europeans will own a mobile phone and, by that time, purchasing a voice-only mobile phone will be impossible.[70] These statistics suggest that sixty-six percent of Europeans will have the potential to engage in e-commerce. To encourage these Europeans to engage in e-commerce, the European Union must provide adequate data protection legislation.

While the development of WAP has provided Internet access to the mobile phone user, similar technologies give service providers the ability to determine the user's geographic location.

C. Location Data through Global Positioning Satellites

Imagine yourself on a relaxing stroll at the beach. As you walk by a hotel, your mobile phone begins to beep. The phone signals that you have a text message. The message reads, "Rooms available. Stop by now and receive a 20% discount at the Sandshell Hotel." Global Positioning System (GPS) chips allow mobile communication networks to give the exact geographic position of their mobile phone users, or technically, the location of their mobile phone. This information is called location data. This data is just one example of how advertisers could use wireless technology to reach their consumers. This example is a small illustration of how location data may be used. Data may also be used to provide traffic information and guidance to drivers.[71] In the near future, location data will become an indispensable part of wireless devices and mobile services.[72]

In fact, the United States has required service providers to include location technology in all mobile phones by October 2001.[73] The United States intends to use location data to assist 911 emergency crews. These emergency crews will use the data to find a caller's geographic location and provide the required assistance.

---

69. Barnard, *supra* note 8, at 14; Yaukey, *supra* note 11.

70. Barnard, *supra* note 8, at 15.

71. Proposed Directive on Electronic Data Protection, *supra* note 20, at 4.

72. Matt Hamblen, *Slippery Road Ahead for Wireless Apps; Analysts Say Loss of Privacy a Potential Hazard for Users, Big Liability for Providers*, COMPUTERWORLD, Oct. 2, 2000, at 10. The Federal Communications Commission has set Oct. 1 of next year as the deadline for carriers to begin providing location services for wireless phones.

73. Anonymous, *supra* note 31; Perine, *supra* note 13.

In recent contemplation of similar legislation, Europe has been researching the feasibility of similar technologies and requirements.

However, one can imagine how this technology brings privacy considerations to the forefront. Consumers could potentially be under constant surveillance.

D. Potential Security Risks Associated with Wireless Internet Access[74]

The European Union has recognized trust and confidence in the on-line community as the key factors affecting consumer behavior.[75] In the United States, the Internet would be used thirty to forty percent more if Americans believed it was more secure.[76] In February of 2000, "hackers" cracked into France's VISA bankcard system which raised questions and concerns about the future of consumer protection in e-commerce.[77] A survey of 100 on-line businesses worldwide found that seventy-two percent of on-line merchants believe consumers would spend more if they did not have to worry about fraud.[78] Erkki Liikanen, European Commissioner for Enterprise and the Information Society, has stated that, "a high level of Internet security must be achieved to build trust amongst businesses and consumers. This is key to the fast take-up of e-commerce."[79]

Consumer trust is a significant concern. Wireless Application Protocol has security issues that may be resolved through proper legislation. However, to create effective legislation, the European Union must attempt to address general and unique security issues associated with the wireless Internet.

Unlike wired Internet connections, a wireless phone communicates with an intermediary while accessing the Internet. This intermediary (the WAP gateway) is on the service provider's premises. In a wired connection, the user connects directly to the Internet site. In a wireless transaction, a third party, specifically the WAP gateway, exists as a middleman in the transaction.

---

74. Although this comment raises security and privacy issues associated with the wireless Internet, this comment will not attempt to discuss preventative security measures developed by the wireless industry.

75. Guttman, *supra* note 6, at 13.

76. Krause, *supra* note 15, at 17.

77. *Id* at 18.

78. Erkki Liikanen, *Europe & eBusiness*, PRESIDENTS & PRIME MINISTERS, July 1, 2000, WL 19413831.

79. *Id.*

These gateway computers are located on the service provider's premises.[80] Some examples of these service providers would be AT&T Wireless, Sprint PCS, and Verizon.[81] Security analysts are mainly concerned with the idea that the business's transmissions will enter another company's premises before it reaches the user.[82] As a result, the business will have less control over the transmission once it is received and processed by the service provider. The main concern is that the user's personal data may be compromised on the service provider's premise.[83]

For a period of 100 milliseconds, the user's requested information is vulnerable.[84] This information is vulnerable at the decryption pause,[85] which occurs when the WAP gateway translates the Internet protocol to the Wireless Application Protocol.[86] For this brief period, any individual with access to the service provider's WAP gateway may access the user's information.[87] At this point, the unauthorized individual can misuse the user's personal information as they would like. Although decryption pause concerns exist, analysts believe that a new version of WAP will eliminate this pause.[88] But until then, the WAP gateway presents this unique security concern.

A possible security concern noted with the wireless Internet is a rogue server intercepting the user's transmission.[89] Although digital signals are difficult to decrypt without the proper software, a compromised computer may be used to receive the user's WAP transmission. Like the legitimate WAP gateway, the unauthorized gateway can process the data for an individual's personal use.[90] These rogue servers would essentially be decommissioned WAP gateways or compromised WAP gateways located on the service

80. Levitt, *supra* note 58.
81. *Id.*
82. *Id.*
83. *Id.*
84. Hamblen, *supra* note 65, at 72.
85. *Id.*
86. *Id.*
87. *Id.*
88. *Id.*
89. Grossman, *supra* note 57, at 36; With the wireless Internet, a mobile phone sends its Internet communications over the airwaves. P.J. Connolly & Jessica Davis, *Can Wireless be Protected?*, INFOWORLD, Nov. 13, 2000, at 46. Over the airwaves, any person may intercept these communications. *Id.* Although digital transmissions are difficult to decrypt or to descramble, the information contained in these transmissions may still be misused, e.g., rogue servers. Robert Grapes, *Security in the Wireless Transaction World*, TELECOMMUNICATIONS AMERICAS EDITION, Sep. 2000, at 34.
90. Grossman, *supra* note 57, at 36.

provider's premises.[91] Unlike the wired Internet environment, rogue servers may intercept WAP transmissions since these wireless transmissions travel through the airwaves.[92] Another unique security concern associated with accessing the wireless Internet is a mobile phone's limited capabilities.[93] Today's mobile phones are severely limited when it comes to bandwidth, memory resources, and battery life;[94] therefore, the goals in wireless are smaller and simpler. These limitations require different security approaches than those developed for wired devices. Wired devices, like desktop computers, are traditionally more advanced and have the ability to provide more complicated security measures. Naturally, when wireless devices were developed, many security measures employed by personal computers were too cumbersome for cellular phones. Many security analysts and companies, after considering these limitations, have explored preventative security measures for the wireless Internet.

Although current European Union legislation has created fundamental rights to privacy and intends to guard the citizens' interest in the processing of their personal data,[95] this data protection legislation may not contemplate the security issues that arise with regards to the mobile wireless Internet.

III. European Union's Data Protection Legislation

Before the recent developments in mobile telephony, the European Union attempted to protect consumers with regard to the processing of their personal data.[96] First, in 1981, the European Union established the fundamental right to privacy for the processing of personal data.[97] These obligations were created during the Council of Europe Convention. Next, in 1995, the European Union established several guiding principles in processing personal data while ensuring the free movement of such

91. *Id.*

92. P.J. Connolly & Jessica Davis, *Can Wireless be Protected?*, INFOWORLD, Nov. 13, 2000, at 46.

93. *Id.*

94. Julekha Dash, *Cost, Reliability Impede Wireless Device Adoption; Potential Users Also Cite Speed, Security Risks*, COMPUTERWORLD, July 3, 2000, at 8; Brian Fonseca, *Wireless Security Concerns*, INFOWORLD DAILY NEWS, June 8, 2000.

95. Data Protection Directive, *supra* note 16, at 31.

96. European Union Commission, *Data Protection: Background Information*, *at* http://europa.eu.int/comm/internal_market/en/media/dataprot/backinfo/info.htm (last visited Jan 18, 2001).

97. Council of Europe Convention of 28 January 1981 for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

data.[98] These guiding principles are embodied in the European Union's Data Protection Directive. In this Directive, the European Union has defined "personal data" as any information relating to an identifiable person,[99] i.e., credit card numbers, social security numbers, and location information. By adopting this Directive, the European Union established the legal framework for the protection of personal data. Finally, in 1998, the European Union adopted a Directive that supplemented the Data Protection Directive. The European Union did this by creating the Telecommunications Directive, which intended to protect the processing of personal data in the telecommunications sector.[100]

In 1981, the Council of Europe Convention established basic principles of data protection.[101] This Convention created obligations for entities that processed data.[102] One of the main principles included in the Convention is the obligation to guarantee the security of data. This obligation can be found in all the data protection laws in Europe.[103]

As information technology developed, the European Union adopted the Data Protection Directive. The European Union realized that information technology was making the process and exchange of data considerably easier.[104] With the data protection laws differing among the Member States, the European Union sought to harmonize the States' national provisions.[105] This Directive requires data controllers to observe several principles in the process and exchange of data. For example, the data processors must have a legitimate purpose for processing personal data[106] and

98. Data Protection Directive, *supra* note 16.
99. *Id.* art. 2.
Article 2 of the Data Protection Directive states:
For the purposes of this Directive:
(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
100. Telecommunications Directive, *supra* note 17.
101. European Union Commission, *supra* note 96.
102. *Id.*
103. *Id.*
104. Data Protection Directive, *supra* note 16, at 1.
105. *See id.*
106. *Id.* art. 6.
Article 6 of the Data Protection Directive states:
1. Member States shall provide that personal data must be:
(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not

processing should be proportionate to that purpose.[107] Data processors also need to process accurate information.[108] If the data is inaccurate, then the processor must take steps to correct this information.[109] The personal data must be relevant for the purpose of processing.[110] These processing principles create a specific framework for Member States to implement into their national law.

Also, this Directive creates guidelines as to when personal data can be processed.[111] For example, personal data can be processed when the data subject has given unambiguous consent after being adequately informed.[112] Data may also be processed for the

---

further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

107. *Id.* art. 6.

108. *Id.* art. 6.

109. Data Protection Directive, *supra* note 16, art. 6.

110. *Id.* art. 6.

111. *Id.* art. 7.

Article 7 of the Data Protection Directive states:

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

112. *Id.* art. 7.

performance of a contract, or when the law requires the processing.[113]

As technology developed, the language of the Data Protection Directive became too narrow. Specifically, the European Union believed this Directive's language would not effectively harmonize the Member States' data protection laws in the telecommunications sector. Therefore, the European Union passed into law the Telecommunications Directive. This Directive concerns the processing of personal data and the protection of privacy in the telecommunications sector.[114] This Directive merely supplements the principles set forth in the Data Protection Directive and introduces new language relevant to public digital mobile networks, or in other words, mobile phone service providers.[115]

Although the Telecommunications Directive's terminology intends to harmonize laws in the telecommunications sector, this same language narrows the scope of data protection in this sector.[116] For example, this Directive extends the Data Protection Directive's guidelines to the telecommunications sector by using language which may limit the definition of "telecommunications" to voice telephony.[117] The problem with the Directive's language is its inability to contemplate recent developments in telecommunications, such as non-voice communications, i.e., electronic messaging, location data, and Internet communications.[118] Recently, the

113. *Id.* art. 7.
114. Telecommunications Directive, *supra* note 17, at 1.
115. *Id.* art. 1.
Article 1 of the Telecommunications Directive states:

> 1. This Directive provides for the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community.
> 2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of legitimate interests of subscribers who are legal persons.
> 3. This Directive shall not apply to the activities which fall outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

116. *See* Proposed Directive on Electronic Data Protection, *supra* note 20, at 2.
117. *Id.* at 2.
118. *Id.* at 2.

European Commission discovered the Directive's shortcomings and addressed these concerns by proposing another directive.[119]

IV. Proposed Data Protection Laws

The European Union, through efforts from Erkki Liikanen, has been aggressively seeking to stimulate e-commerce growth throughout Europe. To fuel this aggressive advance, the European Union has renamed its electronic commerce economy, "e-Europe." Along with this title, the European Union has been developing what it has been dubbed "e-initiatives."[120] These e-initiatives are focused on "an ambitious agenda to push through all remaining electronic commerce legislation by the end of [2000] . . . ."[121] Accordingly, this legislation, by securing consumer trust, will promote e-commerce participation and help the European Union catch the U.S. in the Internet economy. One proposal in the European Union's e-initiative agenda is an Electronic Communications Proposal,[122] which concerns the processing of personal data and the protection of privacy in the electronic communications sector.

The European Commission's proposal seeks to replace the Telecommunications Directive and adapt it to new and foreseeable developments in e-commerce.[123] One way the Commission seeks to adapt its legislation is by making the proposal's terminology technology neutral.[124] Instead of the term "telecommunications," the proposed directive would employ the term "electronic communications."[125] With this neutral language, the Commission intends to protect voice communications and also protect any type of electronic communications.[126] This change would bring WAP transmissions within the proposed directive's ambit. Also, with technology-neutral language, the proposed directive will not limit itself to current technology.[127] The proposed directive's language is

119. *Id.* at 2.
120. Deborah Hargreaves, *Fast Track for E-Commerce Laws: Brussels Sets End-of-Year Deadline to Help Boost EU Internet Economy*, FIN. TIMES, Jan. 27, 2000.
121. *See id.*
122. Proposed Directive on Electronic Data Protection, *supra* note 20.
123. *Id.* at 2.
124. *Id.* at 2.
125. *Id.* art. 2.
126. *Id.* at 2.
127. Proposed Directive on Electronic Data Protection, *supra* note 20, at 2.

broad enough to protect data communications regardless of the technology used.[128]

In addition, the Commission's proposed directive ensures the confidentiality of the mobile phone user's communications.[129] This proposal requires the Member States to implement legislation that prohibits the interception or surveillance of communications without the user's consent.[130] Next, this proposal requires the providers of mobile phone services to inform subscribers, or their customers, that a particular breach of the network's security has occurred.[131] The providers also must inform their customers of the risk and possible remedies involved with such a breach of security.[132]

Not only does the proposed directive protect the mobile phone user's communications, but it also protects the user's location information.[133]

The proposed directive would provide certain guidelines with regard to the processing of location data. For instance, unless the mobile phone user's personal data is anonymous or the user has given consent, the proposed directive would prohibit the processing of the user's location data.[134] When a service provider processes the user's location data, the provider must inform the user of the type of location data it will process, and of the purposes and duration of the processing.[135] The providers must inform the user regarding the transmission of location data to a third party.[136] The Commission, by creating the proposed directive, seeks to prevent the misuse of location data and to ensure the privacy of mobile phone users.[137] This proposed directive is effective since it would provide protection in the privacy and security issues discussed in Part I of this comment.

Although the European Commission has created a proposal that addresses many concerns with upcoming wireless Internet technologies, some Member States' have failed to implement previous forms of data protection legislation, like the Data

128. *Id.* at 2.
129. *Id.* art. 5.
130. *Id.* art. 5.
131. *Id.* art. 4.
132. Proposed Directive on Electronic Data Protection, *supra* note 20, art. 4.
133. *Id.* art. 9.
134. *Id.* art. 9.
135. *Id.* art. 9.
136. *Id.* art. 9.
137. Proposed Directive on Electronic Data Protection, *supra* note 20, at 4.

Protection Directive and the Telecommunications Directive.[138] This failure may be an obstacle to Europe's e-commerce participation.

V. Implementation of the European Union's Data Protection Directives by the Member States

As of January 2001, only ten out of fifteen Member States had implemented some sort of data protection legislation into their national law.[139] In fact, Denmark, France, Germany, Ireland, and Luxembourg may be brought before the European Court of Justice for failing to implement the Data Protection Directive within the deadline established.[140] This Directive provides that, "Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive (95/46/EC) at the latest at the end of a period of three years from the date of adoption."[141] The Directive was adopted on October 24, 1995.[142]

---

138. Data Protection: Implementation of 95/46, *at* http://europa.eu.int/comm/internal_market/en/media/dataprot/law/impl.htm (last visited Jan. 18, 2001).

139. *Id.*

140. *Id.*

141. Data Protection Directive, *supra* note 16, art. 32.

Article 32 of the Data Protection Directive states:

> 1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.
>
> When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.
>
> 2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.
>
> By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.
>
> 3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.
>
> 4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

The Telecommunications Directive, which supplements the Data Protection Directive, also had an implementation deadline of October 24, 1998.[143] Article 5 of this Directive, which deals with the confidentiality of communications, had an implementation deadline of October 24, 2000.[144] Like the previous Directive, some Member States have failed to implement the Telecommunications Directive. Again, the Member State's failure to implement this Directive is another example of the slow, deliberate, methodical nature of the European Union.

VI. Timeliness of Data Protection Legislation

As discussed in Part III, the European Union had developed an ambitious agenda to conclude all remaining e-commerce legislation by the end of 2000.[145] However, at the beginning of 2001, the European Union has yet to bring its proposals into force.[146] The European Union is wasting its "once-in-a-lifetime" opportunity to catch the United States.[147] Although the mobile phone stands as a legitimate successor to the personal computer as the most common

142. *Id.* at 31.

143. Telecommunications Directive, *supra* note 17, art. 15.

Article 15 of the Telecommunications Directive states:

> 1. Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive not later than 24 October 1998.
>
> By way of derogation from the first subparagraph, Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with Article 5 of this Directive not later than 24 October 2000.
>
> When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference at the time of their official publication. The procedure for such reference shall be adopted by Member States.
>
> 2. By way of derogation from Article 6(3), consent is not required with respect to processing already under way on the date the national provisions adopted pursuant to this Directive enter into force. In those cases the subscribers shall be informed of this processing and if they do not express their dissent within a period to be determined by the Member State, they shall be deemed to have given their consent.
>
> 3. Article 11 shall not apply to editions of directories which have been published before the national provisions adopted pursuant to this Directive enter into force.
>
> 4. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive.

144. *Id.* art. 15.

145. Hargreaves, *supra* note 120.

146. *See* Proposed Directive on Electronic Data Protection, *supra* note 20.

147. Barnard, *supra* note 8, at 14.

way to surf the Internet,[148] the Member States seem to implement these directives in slow motion[149].

Even two years after the deadline, some Member States have failed to implement critical data protection legislation.[150] This failure shows the European Union's difficulty with bringing timely legislation into force. The technology sector constantly changes, expands, and develops. Failure to bring timely legislation into force is especially detrimental when the legislation pertains to the technology sector. In fact, the European Union Commission has recognized its decision-making process as being too slow for the technology sector.[151] After some Member States have failed to implement existing data protection directives, it is evident that new directives will be treated similarly. Therefore, the European Union must resolve implementation concerns in its e-Europe agenda.

The EU, through expedited legislation, may resolve its implementation problems. The solution to this conundrum is the doctrine of "direct effect."

VII. Doctrine of Direct Effect[152]

This section will define the doctrine of direct effect and explain its usefulness with regards to European Union directives. Next, this section will discuss ways in which the doctrine may be used to provide consumer trust and confidence in the Commission's Electronic Communications Proposal. The doctrine of direct effect is a judicial doctrine; however, this comment suggests how a legislative provision based on this doctrine will help the European Union avoid the slow implementation of its directives. This provision would protect individuals after the implementation deadline expires. Without this type of provision, the Member States in violation would be brought before the European Court of Justice to decide whether the doctrine of direct effect applies. This provision may eliminate this lengthy delay traditionally associated with the judicial process.

A. Directives and Direct Effect

By its nature, a European Union directive is ineffective

148. *See* Guttman, *supra* note 6, at 11.
149. *See supra* notes 13-14 and accompanying text.
150. *See supra* notes 13-14 and accompanying text.
151. Hargreaves, *supra* note 120.
152. The author would like to thank Professor Larry Catá Backer for his ideas and guidance in this area of European Union Law.

without implementation by the Member States.[153] By definition, a directive is an order to the Member States to implement a European Union policy measure into the states' national legal system.[154] These directives are binding on the Member States and the states must implement them into their national law in whatever way they choose.[155]

Since the European Union promulgates directives as an order to the Member States to implement certain policies, these directives fail to have a binding effect on individuals until the Member States transpose the directives into law. However, the European Court of Justice, through case law, has developed a doctrine which gives individuals the right to rely on directives regardless of their countries' national implementation measures: the doctrine of direct effect.[156]

After a Member State neglects to transpose a directive into its national law by the prescribed deadline,[157] a directive may directly apply to individuals if the directive imposes on an addressee (or Member State) a "sufficiently clear, unconditional, and precise obligation."[158] This obligation must go beyond an obligation for the Member States, but must create rights for the individual. The directive must contain specific guidelines and obligations for direct effect to exist. The directive's language must be such that the Member States have no latitude or discretion in the implementation of the directive's subject matter. In other words, the Member States may implement as they choose; however, they may not alter the legal rights conferred by the directive. If the directive possesses these characteristics, then "individuals to whom that provision applies are entitled to rely on it before the national courts."[159] Like international treaties, a directive that possesses these qualities is said to be "self-executing" in nature.[160] In addition, the Member

153. P.S.R.F. MATHIJSEN, A GUIDE TO EUROPEAN UNION LAW 139 (6th ed. 1995).

154. *Id.* at 139.

155. In fact, the Member States may implement directives as administrative law, just as long as these directives become binding law in the Member States' legal system.

156. Case 26-62, Van Gend en Loos v. Nederlandee Administratie der Belastingen, 1963 E.C.R. 1.

157. MATHIJSEN, *supra* note 153, at 158.

158. Case T-254/97, Fruchthandelsgesellschaft mbH Chemnitz v Commission of the European Communities, 1999 ¶29.

159. Case C-416/96, Nour Eddline El-Yassini v Secretary of State for Home Department, 1999 E.C.R. I-1209, ¶ 32.

160. PAUL CRAIG & GRÁINNE DE BÚRCA, THE EVOLUTION OF EU LAW 179 (1999).

States are liable for refusing to bring the directives into force since by treaty, they are obligated to do so. As a result of this obligation, the Commission may bring the non-complying Member State before the European Court of Justice.

B. A Direct Effect Provision

The Electronic Data Protection Proposal contemplates and reconciles some of the privacy and security concerns associated with the wireless Internet. However, it does not solve the slow implementation concerns of the previous data protection directives. As discussed in Part IV, five Member States have failed to implement the Data Protection and Telecommunications Directives. If these states have failed to implement these previous directives, then they will unlikely transpose a new directive into law in a punctual manner.

With timeliness a serious factor, the European Union should create data protection legislation that includes a "direct effect" provision. Previously, the doctrine of direct effect has been a tool strictly used by the European Court of Justice to allow an individual to rely on an unimplemented directive. However, this comment proposes that the European Commission should create a directive that specifically contemplates this doctrine and specifically provides for this doctrine to take effect through a "direct effect" provision. This legislation will need to fulfill the European Court of Justice's criteria for the imposition of a direct effect. These criteria would require that the data protection legislation impose sufficiently clear, unconditional, and precise obligations on the Member States.

By creating a direct effect provision, the Commission would provide clear legislative intent that timeliness is a crucial factor in the technology sector. Avoiding regulations and legislating a directive, the Commission would allow the Member States to transpose the data protection directive as they wish while protecting the consumers' privacy and security in a timely fashion. The Commission should create a directive with an implementation deadline of one year. If the Member States fail to implement this directive at the end of the year, then the directive will have a direct effect on the citizens of the states.

The Commission's proposal, which is applicable to the electronic communications sector, maintains characteristics consistent with a directive that triggers a direct effect. Since this proposal maintains these characteristics, it stands as a suitable

candidate to accommodate a direct effect provision. First, this proposal confers a fundamental right of privacy and security regarding an individual's electronic communications. Second, this proposal provides clear guidelines to the processing and storage of personal data. Finally, this proposal has an implementation deadline of one year.

To provide a new directive that fosters consumer trust and stimulates e-commerce participation, the Commission should focus on two objectives. First, the Commission should revamp its Electronic Data Protection Proposal to include a direct effect provision. This provision would solve the slow implementation problems that plague technology legislation in the European Union. Second, the Commission, through promoting the "e-initiative" and the "e-Europe" themes, should quickly pass this proposal into a directive.

This proposal coupled with direct effect legislation will likely provide the punctual data protection legislation needed to stimulate e-commerce growth. This punctual legislation is needed since clear and predictable data protection legislation is "vital to build trust and confidence" in the e-commerce economy.[161]

VIII. Conclusion

With the advent of the mobile wireless Internet, Europe is poised to catch the United States' Internet economy; however, current data protection directives by the European Union do not contemplate the potential security and privacy concerns associated with this new technology. Not only are these directives arguably inadequate, but also five of the Member States have still neglected to implement these directives after three years. With these concerns in mind, the European Union must provide technology-neutral directives that will overcome the Member States' proclivity to slowly implement data protection directives.

The European Commission can solve these concerns by revamping its electronic communication proposals. By including a provision that contemplates the doctrine of direct effect, the Commission could ensure consumer protection despite the Member States' national implementation measures. Also, by adopting a directive rather than a regulation, the European Union will provide the Member States with latitude in the transposition of their data protection laws while guaranteeing the timeliness of consumer

161. *See* Barnard, *supra* note 25, at 8.

protection.

Europe has three years to overtake the United States' e-commerce supremacy, and with the aid of a direct effect provision, the European Union has the ability to legislate consumer trust and compete in the e-commerce market with the United States.

Alfred Villoch III