

**Boston University  
Journal of Science & Technology Law**

**Symposium**

Financial Services: Security, Privacy, and Encryption

Thomas W. Cashel, Valerie J. McNevin, Gail Bronson, John Doggett,  
and Michael J. Schmelzer

**Table of Contents**

Speeches.....	[9]
Valerie J. McNevin.....	[9]
Gail Bronson.....	[44]
John Doggett.....	[58]
Michael J. Schmelzer.....	[70]
Question and Answer Session.....	[74]

---

# Financial Services: Security, Privacy, and Encryption†

Thomas W. Cashel, Valerie J. McNevin, Gail Bronson, John Doggett,  
and Michael J. Schmelzer

## Thomas W. Cashel:<sup>1</sup>

1. Thank you for coming to the fourth session of the Internet Law Symposium<sup>2</sup> co-sponsored by the law firm of Testa, Hurwitz & Thibault<sup>3</sup> and the Center for Law and Technology at Boston University School of Law.<sup>4</sup> In directing the Graduate Program for Banking Law Studies at Boston University School of Law, the Morin Center<sup>5</sup> adjusts the curriculum periodically to account for contemporary changes in banking law. We have worked our way through mergers and acquisitions, and the thrift crisis. Now there appears to be another area for which we must

---

† © 1997 by the Trustees of Boston University. Cite to this symposium as 3 B.U. J. SCI. & TECH. L. 4 (1997). Pin cite using the appropriate paragraph number. For example, cite the first paragraph of these proceedings as 3 B.U. J. SCI. & TECH. L. 4 para. 1 (1997) (comments of Thomas W. Cashel). These materials are proceedings from the fourth session of the Internet Law Symposium held at Boston University School of Law on May 15, 1996. For materials from the other sessions, see 3 B.U. J. SCI. & TECH. L. 1-5 (1997).

<sup>1</sup> Thomas W. Cashel is Professor of Law and Director of the Morin Center for Banking and Financial Law Studies at Boston University School of Law.

<sup>2</sup> Other sessions of the Internet Law Symposium are available at 3 B.U. J. SCI. & TECH. L. 1-5 (1997).

<sup>3</sup> Testa, Hurwitz & Thibault is a Boston-based law firm nationally renowned for its leadership in the fields of emerging technology, private equity, and venture capital. For more information on Testa, Hurwitz & Thibault, see *Testa, Hurwitz & Thibault* (visited Mar. 25, 1997) <<http://www.tht.com>>.

<sup>4</sup> Faculty and students at Boston University School of Law's Center for Law and Technology engage in research, education, and public service focused on the role of law in shaping technological progress and the policy issues raised by advances in electronics, communications, robotics, biology, industrial chemicals, and related areas of science and technology.

<sup>5</sup> Boston University established the Morin Center for Banking and Financial Law Studies in 1978.

develop a curriculum. It is interesting to note that in a 1984 case, *Association of Data Processing Services Organizations, Inc. v. Board of Governors of the Federal Reserve System*,<sup>6</sup> then Judge Scalia said that there is a “torrent of recent scientific innovation in the fields of electronics and telecommunications which possess a peculiar capability to destroy the categories of enterprise upon which regulation is based.”<sup>7</sup> We have adopted this quotation as a theme for our analysis of the future of banking law and the tailoring of our curriculum. We have innovated this year with an experimental course in electronic banking and we are learning as we go forward.

2. Banks have always been the repositories of consumer confidence. The consumer relies on banks to have a payment system that is secure and that guarantees privacy. I am sure as we go through our discussion today we will see how the advent of electronic banking is having an impact on those concerns.

3. For those of you who are not banking lawyers, bankers, or people who write about banks, the basis of banking regulation in the United States and in many parts of the world is geographical. The geographical basis for banking regulation is obviously going to be subject to change if we have sites at which people can conduct financial transactions without regard to geography.<sup>8</sup> I am sure that these kinds of issues, which are now keeping the regulators occupied, will be discussed today.

4. Our first speaker is Valerie J. McNevin, a Principal of the Center for Public Trust, and a Kellogg Fellow, specializing in electronic banking and payment systems. Ms. McNevin teaches the current experimental course in international electronic financial services added last semester to the Graduate Program at the Law School.

5. Our second speaker is Mr. John Doggett, Director of Applied Technology at Bank of Boston. He is on the executive committee of the Financial Services Technology Consortium and will talk to us about what banks are doing in the area of security, privacy, and encryption.

6. Our third speaker is Gail Bronson, President of the consulting company, InternetAssist, which specializes in security technology, strategic marketing, and financial services on the Internet. She is also an independent columnist.

7. Our final speaker is Michael Schmelzer, a student at Boston University School of Law. He is the outgoing President of the Technology and Science Law Association which assisted in organizing this symposium.

8. Ms. McNevin will give us an overview of payment systems, legal structure, and various banking issues. Mr. Doggett will tell us what banks are doing in this

---

<sup>6</sup> 745 F.2d 677 (D.C. Cir. 1984).

<sup>7</sup> *Id.* at 697.

<sup>8</sup> See *Global Regulation Gathers Pace*, FIN. REG. REP. (London), May 1, 1995, at 1, available in 1995 WL 9772653.

area. Ms. Bronson will talk about encryption and privacy issues. Mr. Schmelzer will talk about some aspects of money laundering.

**Valerie J. McNevin:<sup>9</sup>**



Valerie J. McNevin

9. The commercial field today is a pretty chaotic environment because we are introducing technology.<sup>10</sup> One of the areas where we are introducing technology, or attempting to introduce technology, and creating an extremely chaotic environment, is into the law schools.

10. My regulatory background is both in telecommunications and in the banking or financial services industries. I have had the opportunity to live through the AT&T divestiture and the savings and loan crisis. When I went through these

---

<sup>9</sup> Valerie McNevin, Esq. is a Principal of the Center for Public Trust and teaches at Boston University School of Law.

<sup>10</sup> See, e.g., John Morency, *So-Called Network 'Standards' Are Only Increasing Intranet Confusion*, COMM. WK., Sept. 9, 1996, at 32 (discussing the confusion arising from uncertain network standards); John Morency, *The Mr. Fix-It of the Year 2000 Computer Crisis*, BUS. WIRE, Oct. 3, 1996, at 1, available in LEXIS, News Library, Curnws File (anticipating a crisis in the year 2000 when computers will not recognize the "00" of the year 2000).

episodes in my practice, I began to realize that there was a significant change in the level of trust and confidence that people had in this country with respect to those particular industries. I had the opportunity two years ago to become a Fellow with the Kellogg Foundation.<sup>11</sup> When I entered into the Fellowship, I asked to do a series of studies on public trust, change, and technology because I could see that technology was coming in as a flood and it was going to have a significant impact, particularly in the telecommunications and financial services industries. The Foundation took that request on and then told me to sit down, fasten my seat belt, and hold on for the ride of a lifetime. And, in fact, that is what has occurred. Over the next 30 minutes I am going to try to give you just a few highlights of the trip that I have taken so far.

11. In my studies, I have spent a good deal of time looking at Chinese law and Chinese philosophy. One of the things that I find interesting is that the Chinese strongly believe that business is war and that the marketplace is the battlefield.<sup>12</sup> Winn Schwartau published a book a couple of years ago called *Informational Warfare*.<sup>13</sup> It is very important for us to start out this afternoon talking about what is happening in terms of the Internet, technology, and electronic banking within the concept of "information warfare." There is an ancient Chinese treatise called *Master of the Hidden Storehouse*.<sup>14</sup> Many of the military treatises that came out of China were actually treatises dealing with business. In this particular treatise, the old sage is teaching his student about war, and he says, "War comes from above and there is never a time when it is not in operation. When you look into the signs of war, they are in the mind."<sup>15</sup> Certainly that sums up what is occurring in the commercial field today. Even today when we look at the title for this session, "Privacy, Security, and Encryption," we ask ourselves what these words signify. These are words of war. In fact, we are entering into a cultural change, a paradigm shift, when instead of looking at business in terms of trust and confidence, we are looking at it in terms of protection and security. The question is protection from what and from whom.

---

<sup>11</sup> The Kellogg Foundation was established in 1930 "to help people help themselves through the practical application of knowledge and resources to improve their quality of life and that of future generations." See *About the W.K. Kellogg Foundation* (modified Feb. 15, 1996) <<http://rhetoric.agri.umn.edu/~vision/kellogg.html>>.

<sup>12</sup> See THE WILES OF WAR 60 (San Haichem trans., Foreign Languages Press 1991); THUNDER IN THE SKY: SECRETS ON THE ACQUISITION AND EXERCISE OF POWER vii (Thomas Cleary trans., Shambhala 1993).

<sup>13</sup> WINN SCHWARTAU, INFORMATIONAL WARFARE: CHAOS ON THE ELECTRONIC SUPERHIGHWAY (2d ed. 1994).

<sup>14</sup> MASTER OF THE HIDDEN STOREHOUSE, *translated in* THUNDER IN THE SKY, *supra* note 12, at 99.

<sup>15</sup> *Id.* at 158.

12. On a global scale, and particularly on a domestic scale, it is important to look at what is happening in the criminal element. On the domestic level, a significant amount of the activity that is occurring on the Internet today is being tapped.<sup>16</sup> In other words, a significant number of messages that go across the Internet are being siphoned off by someone other than the sender or the intended receiver. In this country last year alone we experienced credit card fraud of over \$860 million.<sup>17</sup> We have a substantial amount of counterfeit currency circulating in the economy today.<sup>18</sup> We are not even talking about cellular fraud, but that has significantly increased over the last couple of years.<sup>19</sup> The untaxed economy in this country exceeds \$1 trillion.<sup>20</sup> On a global scale, we know that we lost nearly \$100 billion to Japan, Germany, and China last year as a result of industrial espionage or piracy.<sup>21</sup>

13. Another interesting phenomenon is occurring. Several years ago Japan did not have any sizeable credit card fraud in their country.<sup>22</sup> Today, because of the opening up of their system and the escalating use of credit cards around the world, credit card fraud in Japan is now almost equal to that of the United States.<sup>23</sup> There are countries that take information security and privacy very seriously. United States Trade Representative, Mickey Kantor, has stated that "[b]ribery and corruption are insidious problems. They are a virus threatening the health of the

---

<sup>16</sup> For a discussion of the various risks of electronic communication, see Frank Barbetta, *Security Ignorance Remains Bliss for Most Users*, BUS. COMM. REV., July 1, 1996, at 33.

<sup>17</sup> See Judith Schoolman, *Retailers Deal with Card Fraud*, STAR LEDGER (Newark, N.J.), Nov. 10, 1995 (reporting that the U.S. Office of Consumer Affairs estimates annual credit card fraud exceeds \$3 billion).

<sup>18</sup> See Ralph Vartabedian, *U.S. Responds to Rising Threat of Counterfeiters*, L.A. TIMES, Sept. 25, 1995, at A1.

<sup>19</sup> See, e.g., *Wireless Industry Salutes U.S. Secret Service for One of Nation's Biggest Cellular Fraud Busts*, PR NEWSWIRE, Sept. 11, 1995, available in LEXIS, News Library, Curnws File (estimating the loss from cellular fraud at \$1.32 million per day); *Cellular Fraud: Motorola Taking Initiative to Fight Cellular Fraud with Halt!*, EDGE, July 17, 1995, available in 1995 WL 8798885 (estimating the cost of cellular fraud at nearly \$1.5 million per day).

<sup>20</sup> See *Fall River Businessman and Teacher Hit with \$10,000 Fine and Home Confinement for Paying Workers Under-the-Table*, U.S. ATTORNEY SAYS, PR NEWSWIRE, Sept. 19, 1995, available in LEXIS, News Library, Curnws File.

<sup>21</sup> See 142 CONG. REC. S737 (daily ed. Feb. 1, 1996) (statement of Senator Kohl).

<sup>22</sup> See Richard Lloyd Parry, *How Mr. Cheese Broke Japan's Bond of Trust*, INDEPENDENT (London), June 16, 1996, at 1.

<sup>23</sup> See *Japanese Issuer Selects HNC Fraud Software*, AM. BANKER, Aug. 8, 1996, at 11.

international trading system."<sup>24</sup> We have a global problem on our hands that requires a global response. It requires a harmonized response from different countries and their legal structures.

14. One key to understanding this whole process is the concept of convergence. Convergence is occurring both in the telecommunications industries and in the financial services industries.<sup>25</sup> The telecommunications industry has several goals to reach by 2005.<sup>26</sup> One goal is access.<sup>27</sup> They want all of us to be able to access communications wherever we are in the world. The second goal is availability.<sup>28</sup> They want us to be available via a communications device wherever we might be. We can see this through the use of beepers, cellular phones, and the faxes that are available on your wrist watch. The third goal is inter-operability.<sup>29</sup> They want all telecommunications systems and devices to be able to talk to one another in a common language.

15. The financial services industry is also going through a convergence. They want us to have access to our money wherever we might be in the world. And they want our money to be available to us no matter where it might be housed or what function it is performing. I am sure all of you are aware of the new concept that a portion of our social security be available to invest directly.<sup>30</sup> The other portion of it, of course, would be set aside as sacred, at least for the moment. They want money to be inter-operable, so that there are no barriers to the conversion of money or currency exchange problems.

16. What kind of force is this? The only way I can explain this convergence-force is to analogize it to the western part of the United States during the melt-off of the winter snowfall, coming down into the different tributaries and streams, and

---

<sup>24</sup> 142 Cong. Rec. S1992 (daily ed. May 13, 1996).

<sup>25</sup> See *MTA-EMCI Projects Dramatic Growth in 'Bundled' Telecommunications Services*, PR NEWSWIRE, Aug. 13, 1996, available in LEXIS, News Library, Curnws File.

<sup>26</sup> See *Hearings Before the Subcomm. on the Departments of Commerce, Justice, and State, the Judiciary and Related Agencies of the House Appropriations Comm.*, 104th Cong. 376 (1996) (comments of Clarence L. Irving, National Telecommunications and Information Administration) (discussing several goals including universal access and improved spectrum management).

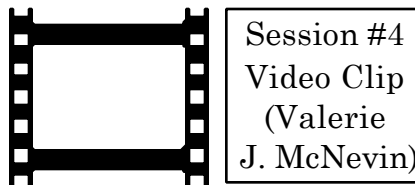
<sup>27</sup> See *id.*

<sup>28</sup> See *id.*

<sup>29</sup> See *id.* at 387.

<sup>30</sup> See generally CONGRESSIONAL BUDGET OFFICE, *BABY BOOMERS IN RETIREMENT: AN EARLY PERSPECTIVE* (1993) (proposing liberalizing social security to allow some private investments).

converging into the river where rapids are created. This is a raw power. It is very chaotic and difficult to negotiate and navigate.



17. This is the era that we are entering in terms of the convergence of the telecommunications and the financial services industries. This convergence grows even stronger when you begin to realize that the old barriers between banks, and securities and insurance firms are coming down. They are coming down because of the force of the delivery mechanisms that are available through the advancement of technology through telecommunications.

18. In addition, we have three trends that are beginning to merge strongly in the commercial field. The first is EDI, or electronic data interchange,<sup>31</sup> which over the last 10 years has seen a rapid escalation in the commercial field.<sup>32</sup> The second trend is electronic fund transfers. An increasing percentage of the money exchanged daily in the United States is transferred via an electronic fund transfer system.<sup>33</sup> The final and new trend is electronic benefit transfer systems.<sup>34</sup> If you are a welfare recipient, a social security recipient, or anyone who is entitled to money from the government, then it is going to be transmitted to you through an electronic transfer system.

19. One projection that I saw recently that I have some difficulty with, and that I find to be rather optimistic, if not staggering, is that hundreds of billions of

---

<sup>31</sup> Electronic data interchange is the exchange of data and documents between different users. See IBM DICTIONARY OF COMPUTING 231 (George McDaniel ed., 1994) [hereinafter IBM DICTIONARY].

<sup>32</sup> See Paul Taylor, *Towards a Dream Market*, FIN. TIMES, Sept. 4, 1996, at 3 (noting \$130 billion worth of goods were handled through EDI in 1995).

<sup>33</sup> But see Jim McTague, *Fears at the Fed: Its Payment System Meets the Internet*, BARRON'S, Dec. 11, 1995, at 29 (reporting that only five percent of worldwide financial transactions are electronic).

<sup>34</sup> See, e.g., Jeffrey Kutler, *Smart Card Veteran from Gemplus Joins Md. Consulting Firm*, AM. BANKER, Aug. 21, 1996, at 10 (noting the use of electronic benefit transfer systems); Brian Ford, *Firm Given Food Stamp, Welfare Pact*, TULSA WORLD, Aug. 7, 1996, at A11 (discussing the utility of electronic benefit transfer systems); Beth Piskora, *EBT Professor Sues U.S. Over Rules Favoring Banks Series*, AM. BANKER, Apr. 25, 1996, at 6, 6-7 (discussing legal obstacles to electronic transfer benefit systems).



dollars worth of goods and services will be purchased over the Internet by the year 2000.<sup>35</sup> They are projecting that \$50 billion alone will be spent in terms of processing transaction costs.<sup>36</sup>

20. Hyperion<sup>37</sup> is a organization that came up with the idea of Mondex.<sup>38</sup> They were concerned that as technology and telecommunications progressed, banks would become outdated as a delivery service.<sup>39</sup> So they began to think about how banks could morph into the technology age. They utilized an old Chinese stratagem. Again, there are 36 strategies in the Chinese military treatises that can be applied to competition in the marketplace.<sup>40</sup> Stratagem number seven talks about “creating something out of nothing,”<sup>41</sup> which is exactly what Hyperion came up with for Mondex. Mondex is a type of smart card. It is one of the types of electronic money that is out and available.

21. What happened when Mondex and Hyperion looked at money was that they looked at the payment systems available to consumers today. The first one they looked at is what is called a “pay-later” system, or as we know it, the credit card system.<sup>42</sup> That is really a pretty young system. Even though it is an ancient tool, it is really only 45 years old in this country.<sup>43</sup> They began to look at how it

---

<sup>35</sup> See Penny Lunt, *Payments on the 'Net: How Many: How Safe?*, A.B.A. BANKING J., Nov. 1995 at 46, 46 (estimating \$600 billion in retail Internet transactions by the year 2000); Wendy Taylor & Marty Jerome, *Mint a Million*, PC COMPUTING, Oct. 1996, at 73 (stating that forecasts for online sales by year 2000 range from \$6.6 billion to \$400 billion).

<sup>36</sup> See Visa, *MasterCard Look for a Model for Billing Internet Users for Transactions Costing Cents Rather than Dollars*, COMPUTERGRAM INT'L, Dec. 15, 1996, at 1, available in 1996 WL 13465390.

<sup>37</sup> For more information on Hyperion, see *Organisation* (last modified Aug. 14, 1996) <<http://www.hyperion.co.uk/pub/pn-organisation.html>>.

<sup>38</sup> Mondex is a stored value card that has been launched in the United Kingdom and Canada. See *Electronic Cash Will Change Everything* (last modified Aug. 13, 1996) <<http://www.hyperion.co.uk/pub/library/PRLibrary/pr003-van9601.html>>.

<sup>39</sup> See Adam Zagorin, *Cashless, Not Bankless Financial Institutions Are Trying to Master the Technology that Could Render Some Obsolete*, TIME, Sept. 23, 1996, at 52, 52.

<sup>40</sup> See THE WILES OF WAR, *supra* note 12, at 60.

<sup>41</sup> *Id.* at 67.

<sup>42</sup> “A credit card allows its holder to buy on credit from stores, restaurants, and other providers of goods and services.” 5 ACADEMIC AMERICAN ENCYCLOPEDIA 336 (1994).

<sup>43</sup> The first credit card was issued by Diner's Club in 1950. See *Variety*, STAR TRIB. (Minneapolis-St. Paul), Sept. 29, 1996, at 1E.

penetrated so quickly and changed society in terms of payment preferences and consumer choices.

22. The second payment system that Mondex and Hyperion looked at was the “now system,” or as we know it, the cash system. Typically the tools for that system are cash, check, or debit cards. They looked at how well these tools had penetrated the system--particularly the debit card because it is plastic--and the changes that the debit card makes in consumer choices.<sup>44</sup>

23. The next system that they found interesting was the “pay-before” system. Its tool is called a stored value card.<sup>45</sup> This system is used by transit authorities.<sup>46</sup> It is also used in the long-distance telephone card industry.<sup>47</sup> They realized that it was a payment system that had not been sufficiently utilized. Much activity could now be generated through the use of a stored value card that previously went to systems utilizing a credit or debit system.

24. Next, they looked at the qualities of money. What would electronic money need to have in order to replicate physical cash? There are several necessary qualities that electronic money would have to have. It would need to be stable, transferable, and recognizable. In other words, to be able to do business together, consumers and merchants would have to be willing and able to recognize it as money. It would need to be durable, as opposed to being perishable, and it would need to be portable. Furthermore, it must not be heavier than physical cash. Otherwise, consumers would not choose to use it. Finally, and most importantly, it would need to be anonymous. In fact, just last year at a cryptographer's conference, the foremost concern for everyone was whether the new money could be used in verifiable, yet untraceable and anonymous transactions.<sup>48</sup>

25. There is much debate and concern about electronic money, or digital cash. One Internet executive sounded a warning, saying that digital cash is a threat to every government on the planet that wants to manage its currency.<sup>49</sup> Obviously,

---

<sup>44</sup> See Cheryl Wetzstein, *Will Debit Cards Make Cash Obsolete?*, WASH. TIMES, Apr. 16, 1991, at C1.

<sup>45</sup> See Andrea McKenna, *Bankers Urged to Get Early Edge on Stored Value Cards*, 18 BANK LETTER, at 1 (1994).

<sup>46</sup> For example, Washington, D.C. uses an automated fare collection system based on stored value cards. See Emily Sacher, *Prepaid Ticket to Ride in the Works for MTA*, NEWSDAY, May 27, 1993, (Business), at 49.

<sup>47</sup> See Pablo Galarza, *Call-ectible*, INVESTOR'S BUS. DAILY, Oct. 28, 1994, at A4 (discussing increasing availability of phone cards).

<sup>48</sup> See *OECD Meeting Makes Progress on Cryptography Guidelines*, OECD News Release (last modified Oct. 1, 1996) <[http://www.oecd.org/news\\_and\\_events/release/nw96-87a.htm](http://www.oecd.org/news_and_events/release/nw96-87a.htm)>.

<sup>49</sup> See Kelly Holland & Amy Cortese, *The Future of Money*, BUS. WK., June 12, 1995, at 66

there are concerns for central banks involving their rules and their functions.<sup>50</sup> Eugene Ludwig, the head of the Office of the Comptroller of the Currency (“OCC”) for this country, said earlier this month that while some concern about electronic money is understandable, an electronic money meltdown is unlikely in the foreseeable future.<sup>51</sup> If you study his statement carefully you will see that it is a very limited, restricted statement with which I agree, to some extent. Mr. Ludwig's statement, however, only includes electronic money as a consumer medium on the Internet and does not look at the full perspective.

26. It is important to consider electronic money in terms of electronic funds transfers, electronic data interchange, and electronic benefits transfer on a global level. It is happening right now. Consider a global time line. In 1887, a reformist lawyer from Massachusetts by the name of Edward Bellamy wrote a book called *Looking Backward*.<sup>52</sup> In that book he prophesized shopping malls, electronic broadcasting, electric lights, and the credit card.<sup>53</sup> Plastic did not exist back then, so he could not foresee that, but he did see what he called pasteboard or a cardboard card that literally took the place of cash.<sup>54</sup>

27. Bellamy's vision has become a reality. The integrated circuit chip (“IC”)<sup>55</sup> is what sits inside the smart card or Mondex, a type of smart card.<sup>56</sup> A smart card looks and operates like a credit card, but it functions like a computer because it has a microprocessor and an IC chip.<sup>57</sup> In the early 1980s, electronic money and electronic funds transfers hit the news<sup>58</sup> and became the banking hope of the future.

---

(quoting David E. Saxton, Executive Vice-President of Netl, an electronic check communication company).

<sup>50</sup> See Olaf de Senerpont Domis, *Ludwig: Excessive Rules Would Stifle Electronic Banking*, AM. BANKER, May 9, 1996, at 2.

<sup>51</sup> See *id.*

<sup>52</sup> EDWARD BELLAMY, *LOOKING BACKWARD* (1887).

<sup>53</sup> *Id.* at 87.

<sup>54</sup> See *id.*

<sup>55</sup> An integrated circuit is a small piece of semiconductive material that contains interconnected miniaturized electronic circuits. See IBM DICTIONARY, *supra* note 31, at 347.

<sup>56</sup> See Rebecca Cox, *Smart-card Industry Rallies to Gain Support for Its Technology*, AM. BANKER, May 31, 1989, at 9.

<sup>57</sup> See *id.*

<sup>58</sup> See, e.g., *Paying for Gas Without an Attendant*, N.Y. TIMES, Jan. 4, 1983, at D5 (predicting widespread use of debit cards at service stations); Robert A. Bennet, *Banks Will Link Cash Machines*, N.Y. TIMES, Apr. 8, 1982, at D1 (discussing the introduction of Plus, the first network to link the

Unfortunately, American consumers did not take to it very well, and so banks left it aside.<sup>59</sup> In the meantime, other countries did look at it seriously, especially those countries that did not have much time or money invested in a payment system or telecommunications infrastructure.<sup>60</sup>

28. European and Asian countries got very excited about electronic money.<sup>61</sup> Most, if not all, countries have some sort of a pilot project under way right now that deals with smart cards or electronic money. Mondex will be operating a significant pilot project this year in Ontario.<sup>62</sup> In China, a very interesting process is occurring. It is called the Golden Card Project and VISA International is involved.<sup>63</sup> They hope to have 200 million credit or debit cards in operation in China by 2003.<sup>64</sup> That may seem like a drop in the bucket to us considering their total population, but understand that the present credit card industry in the United States is saturated at hundreds of millions of cards.<sup>65</sup>

29. Another interesting area is South Africa, where they now have the first biometric pension fund system in which they literally come out with a truck and scan fingerprints or retinas and distribute electronic benefits via a biometric identification system.<sup>66</sup> They are now looking at other ways to utilize a biometric system including DNA mapping.<sup>67</sup>

---

ATM services of multiple banks).

<sup>59</sup> See *Catching Up with Smart Cards*, AM. BANKER, Sept. 13, 1989, at 8.

<sup>60</sup> See *Smart Card Directory Update*, AM. BANKER, May 17, 1989, at 6 (“[M]ost significant smart card advances are outside the United States.”).

<sup>61</sup> See *Catching Up With Smart Cards*, *supra* note 59, at 8.

<sup>62</sup> See *Canadian Banks Take Part in Cash Card Purchase*, CALGARY HERALD, July 19, 1996, at 1; Valerie Block, *NatWest Creation Mondex Isn't Fazed by Fleet Deal Series*, AM. BANKER, Dec. 21, 1995, at 17.

<sup>63</sup> See *Living on Credit*, CHINA ECON. REV., Apr. 1, 1996, at 29, available in 1996 WL 9692194.

<sup>64</sup> See *id.*; see also *Schlumberger to Aid in Chinese Project*, AM. BANKER, May 2, 1995, at 18.

<sup>65</sup> VISA and MasterCard have 442 and 300 million cards in circulation respectively. *Cf. Security is Going On Line MasterCard and Visa Agree on a Standard*, RECORD (New Jersey), Feb. 2, 1996, at B3.

<sup>66</sup> See Matt Barthel, *Interbold Boosting Its Research On High-Tech PIN Alternatives*, AM. BANKER, Oct. 7, 1993, at 16.

<sup>67</sup> See Ira Breskin, *Computers & Technology Biology-Based Identification Forms Security System Niche: Is Biology the Growth Branch of Security?*, INVESTOR'S BUS. DAILY, Jan. 17, 1996, at A6.

30. What is happening with the international legal structure? At this time there are really only two things happening. The Organisation for Economic Cooperation and Development (“OECD”) is considering guidelines on the security of information systems that handle encryption and cryptography.<sup>68</sup> GATT has an understanding on commitment to financial services which, interestingly enough, says that members will freely distribute and exchange technologies related to financial services.<sup>69</sup> Does that also include encryption, and, if so, what happens to export control? Last year Canada came out with very good privacy legislation.<sup>70</sup> The European Union came out with a directive on privacy as it relates to databases.<sup>71</sup> The directive reads that if a country does not have sufficient standards with respect to the protection of private information in databases, the European Union will not trade information with that country.<sup>72</sup>

31. On the federal level in the United States, not much has occurred. We have the Electronic Funds Transfer Act that really deals with consumer transactions.<sup>73</sup> Regulation E gives the Federal Reserve the right to regulate those transactions.<sup>74</sup> We also have Uniform Commercial Code article 4A which deals only with commercial credit transactions.<sup>75</sup> Recently, the OCC promulgated some interpretive rules allowing, for the first time, national banks to sell and market excess capacity in computer equipment and computer lines.<sup>76</sup> Last year, S. 1726

---

<sup>68</sup> The OECD issued final cryptography guidelines on March 27, 1997. *See Cryptography Policy Guidelines* (last modified Mar. 27, 1997) <[http://www.oecd.org/dsti/iccp/crypto\\_e.html](http://www.oecd.org/dsti/iccp/crypto_e.html)>.

<sup>69</sup> Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations, Apr. 15, 1994, UNDERSTANDING COMMITMENTS IN FINANCIAL SERVICES, 33 I.L.M. 1260 (1994).

<sup>70</sup> *See Access to Information Act*, R.S.C., ch. A-1, § 19(1) (1995) (Can.).

<sup>71</sup> *See Amended Proposal for a Council Directive on the Legal Protection of Databases*, 1993 O.J. (C 308) 1, 8.

<sup>72</sup> *See id.*

<sup>73</sup> 15 U.S.C. § 1693g(a) (1994) (limiting consumer liability for an unauthorized electronic funds transfer to \$50).

<sup>74</sup> 12 C.F.R. § 205.1 (1996).

<sup>75</sup> *See generally* U.C.C. § 4A-103 (including electronic instructions in payment orders); § 4A-201 (defining security procedures for electronic fund transfers); § 4A-202 (defining procedures for authorized and verified payment orders); § 4A-204 (providing procedures for refund for unauthorized payment orders).

<sup>76</sup> Interpretive Rulings of the Office of the Comptroller of the Currency, 60 Fed. Reg. 11,924, 11,926 (1995).

was introduced into legislation and would have opened up United States markets for strong encryption products.<sup>77</sup> Another big issue has arisen involving key escrow.<sup>78</sup>

32. On the state level, again not much has occurred. Utah came out with the very first Digital Signatures Act<sup>79</sup> two years ago. The Utah Digital Signatures Act is a 1950s or 1960s solution to a 1990s and beyond problem. The California Digital Signatures Act is an interesting and innovative prototype.<sup>80</sup> It allows for flexibility and innovation in the area. It does not relate just to encryption and to the public/private key escrow agreement.

33. The Colorado Genetic Privacy Act,<sup>81</sup> at first glance, does not look like it has anything to do with financial services. It, however, includes the Human Genome Diversity Project.<sup>82</sup> Colorado became concerned about people engaged in genetic testing. If a test concludes that a person might have a DNA proclivity towards particular diseases later in life, she may not be able to get insurance or a home mortgage. Colorado put forward the Genetic Privacy Act so that this kind of information could not be used against a consumer.<sup>83</sup> This is a trend of things to come.

34. The major issue of trust can be analyzed from a “top-down five-rings” perspective, in which we look at things from a global scale and on a systems basis. This analysis reveals that the financial services industry in this country is becoming

---

<sup>77</sup> S. 1726, 104th Cong. (1995).

<sup>78</sup> See Dorothy E. Denning, *Edited Comments Concerning Regulating State Access to Encrypted Communications*, 1994 ANN. SURV. AM. L. 415, 416 (1994).

<sup>79</sup> UTAH CODE ANN. § 46-3-101 (1993 & Supp. 1996). Digital signatures are an encryption technique used to verify a message sender’s identity. See ROBIN WILLIAMS & STEVE CUMMINGS, JARGON, AN INFORMAL DICTIONARY OF COMPUTER TERMS 152 (1993).

<sup>80</sup> CAL. GOVT CODE § 16.5 (West Supp. 1996) (defining a digital signature as “an electronic identifier, created by computer, intended by the party using it to have the same force and effect as a manual signature.”).

<sup>81</sup> COLO. REV. STAT. ANN. § 10-3-1104.7 (West 1996).

<sup>82</sup> See § 10-3-1104.7(5); The Human Genome Diversity Project, now under the Human Genome Organization, uses scholars throughout the world to document genetic variations in the human species. See Michael J. Malinowski & Maureen A. O’Rourke, *A False Start, The Impact of Federal Policy on the Genotechnology Industry*, 13 YALE J. ON REG. 163, 191 (1996).

<sup>83</sup> COLO. REV. STAT. ANN. § 10-3-1104.7(1)(c) (stating the goal of the law is to “protect individual privacy and to preserve individual autonomy with regard to the individual’s genetic information”).

hugely, if not solely, dependent upon the public switch network.<sup>84</sup> The public switch network is the lifeblood of the United States economic system, and within it there is the EMP, or the electromagnetic pulse.<sup>85</sup> The military considers it the most critical threat to the security of all information systems including the financial services industry.<sup>86</sup> It can be disrupted by jamming signals, and computer chips are far more vulnerable to this disruption than old fashioned radio tubes. This boils down to the concern that we have with regard to the trust zone.<sup>87</sup>

35. Basically, the trust zone is a concept that concerns the Center for Public Trust because when converging the financial and communications sectors of a person's life, the two most vulnerable areas of a consumer's economic life are married. This creates an opportunity for an extreme destruction of confidence in our system. John Adams said that there are two pillars to a free market system: democracy and a sound financial system, and that democracy is usually short-lived and ends up committing suicide.<sup>88</sup> The *Washington Post* published a series of articles arguing that in the course of one generation this country has reversed its position.<sup>89</sup> In the 1960s most people in this country felt that they could trust their government, banks, military, schools, and police.<sup>90</sup> Today, there is a lack of trust.

---

<sup>84</sup> See Norm Alster, *Cascade Profits From the Boom In Telephone Data Transmission*, INVESTOR'S BUS. DAILY, Jan. 8, 1996, at A8. The public switch network is a switch network providing a circuit to many customers. See IBM DICTIONARY, *supra* note 31, at 545.

<sup>85</sup> The electromagnetic pulse is an electromagnetic envelope surrounding the earth. See *Data Communications Glossary*, DATA COMM, Jan. 1, 1985, at 97. An electromagnetic field pulse can be used to produce an effect similar to a lightning strike and can have severe effects on computers and telephone lines. See Carlo Kopp, *The E-Bomb: A Weapon of Electrical Mass Destruction* (visited Feb. 3, 1997) <[http://www.infowar.com/mil\\_c4i\\_c4i8.html-ssi](http://www.infowar.com/mil_c4i_c4i8.html-ssi)>.

<sup>86</sup> See generally *Hearing on Information Warfare and the Security of the Government's Computer Networks before the Permanent Investigations Subcomm. of the Senate Governmental Affairs Comm.*, 104th Cong. 3 (1996) (testimony of John Deutch, Director of CIA) (discussing the national security threats associated with computer security); see also 141 CONG. REC. S12,166 (daily ed. Aug. 10, 1995) (statement of Senator Bingaman) ("[A] rogue nation . . . could generate a theatre atmospheric disturbance electromagnetic pulse, disrupt signal propagation and, frankly, destroy much of our military communications systems.").

<sup>87</sup> See *Pentagon Settles Suit, Will Curtail Electromagnetic Pulse Tests*, SAN DIEGO UNION-TRIB., May 15, 1988, at A2.

<sup>88</sup> See Letter from John Adams to John Taylor (Apr. 15, 1814), in 6 THE WORKS OF JOHN ADAMS 484, 484 (Charles F. Abrams ed., 1851).

<sup>89</sup> Richard Morin & Dan Balz, *Americans Losing Trust in Each Other*, WASH. POST, Jan. 28, 1996, at A1.

<sup>90</sup> See *id.*

We should try to figure out ways to change that and move back out of an information warfare culture to one of trust and confidence in the safety and soundness of our system.

36. Some disconcerting trends include the transfer of risk, cost, and responsibility on to the consumer and away from banks or merchants. In addition, we will have a continued disintermediation, or the removal of intermediate parties, in financial services. For instance, Spring Street is a small microbrewery that recently did an initial public offering on the Internet and raised \$1.6 million without the help of underwriters.<sup>91</sup> This is just the beginning of disintermediation in the securities market.

37. Technology requires standardization, and as we move forward with electronic data transfer, electronic benefits transfer, and electronic funds transfer, we will require considerable global standardization. In addition, we will be relying more on artificial intelligence systems and intelligence enhancement systems. That again will cause a need to standardize our formats and to build a common language for our technology.

38. Consider the erosion of central banks. Escalating crime will continue to be a trend, particularly in those cultures that have not experienced this kind of financial crime in the past. We have a significant erosion of the tax base and money laundering. Most important is the conflict of rights that is going to occur in terms of privacy versus personal and national security.

39. Are there any strategies for regulatory reform? We need to be looking at the reasons why we are getting information. Who is getting the information? What is the process of obtaining, editing, storing, and accessing the information? We need to look at the uses of information. Are we getting information because of the regulatory requirement, or to make a market and target the consumer?

40. Regulatory reform is a major issue, particularly in terms of banking. People believe that they have privacy when it comes to banking records, banking life, and economic life. This is not the case. It is a misperception that many consumers are just now beginning to recognize.<sup>92</sup> We have to make a distinction between security--personal and national--and our international obligations in terms of moving forward into a free market. Consider safety and soundness within the banking system. Safety and soundness now include the public switch network and how banks are addressing security as they introduce their systems to the Internet. Consider trust and liability. You are guilty in cyberspace until you prove yourself

---

<sup>91</sup> See Udayan Gupta, *Microbrewery Uses the Internet to Post Circular on Its IPO*, WALL ST. J., Feb. 24, 1995, at B5; see also *About IPO Trade, Inc.* (visited Mar. 31, 1997) <<http://www.ipotrade.com/about.htm>> (discussing the Spring Street offering).

<sup>92</sup> See *Panel Urges Tough Action Against Rogue Banks*, THOMSON'S INT'L BANKING REG. AM., Oct. 12, 1992, available in 1992 WL 2751140.



innocent. This has become a tremendous burden for the consumer. Jurisdiction, obviously, is also a major issue when you are dealing with the Internet.<sup>93</sup> Another major issue is alliances. We are beginning to see international alliances developing, particularly with large telecommunications firms like AT&T, IBM, and major United States banks.<sup>94</sup> This eventually becomes an antitrust issue.

41. Finally, consider disenfranchisement. We have two classes of people in the technology revolution: those that have technology know-how and access, and those that do not. There is concern about a new kind of red-lining that may result. The challenge we see is building trust between government, people, and commercial entities.

42. Consider twenty-first century thinking skills. These are part of the teaching tools that are going to be utilized in higher academia. Law schools train students to think simply in a linear, logical manner. We need to start thinking in a lateral manner. Lawyers need to be particularly adaptive. A lawyer needs to understand her client's situation. She needs to be strategic and creative with her client. We are going to have to develop new structures. Jefferson said that the structure of government should change and not remain the same.<sup>95</sup> It should change as the dictates of those being governed determine that it needs to be changed. We have to be flexible, agile, and critical in our thinking. Most of all, we have to be cross-disciplinary.

43. Banking law is no longer restricted to a certain area. We have to take aspects of the law from almost every area to look at impacts on financial services and how financial services are going to change in the future. We are redefining the business of banking, and as a result, we are redefining the law that governs that business. I leave you with this thought. If in the West, time is money, and in the East, money is war, are we at war all the time?

---

<sup>93</sup> Several cases have recognized personal jurisdiction in the end-user's location. *See* *Inset Sys., Inc. v. Instruction Set, Inc.*, 937 F. Supp. 161, 165-66 (D. Conn. 1996); *Maritz, Inc. v. Cybergold, Inc.*, No. 4:96cv01340, 1996 U.S. Dist. LEXIS 14978, at \*22 (E.D. Mo. 1996). *But see* *Bensusan Restaurant Corp. v. King*, 937 F. Supp. 295, 299 (S.D.N.Y. 1996).

<sup>94</sup> Unibex is an electronic business-to-business commerce service that includes members such as AT&T, IBM and Chase Manhattan Bank. *See* Chris Jones, *Commerce Vendors Plug in to Network Transaction Systems from Vendors, Banks, Others Work Together Over `Net*, INFO WORLD, Dec. 2, 1996, at 1, available in 1996 WL 14455579.

<sup>95</sup> *See* Letter from Thomas Jefferson to Samuel Kercheval (July 12, 1816), in *THE PORTABLE THOMAS JEFFERSON* 552, 558-61 (M. Peterson ed., 1975).

**Gail Bronson:**<sup>96</sup>

44. Security on the Internet and safe financial communications are important current issues. The Internet was created to share information freely among universities and government entities,<sup>97</sup> and not for conducting clandestine information exchanges. Therefore, the challenge is to retool the system to fit a purpose counter-intuitive to its original definition. Without security, the Internet would never be a viable communications tool for financial services and electronic commerce.<sup>98</sup> Not only would it fail to foil potential criminal activities, but more importantly, it would be impossible to establish and maintain the trust and loyalty of corporate consumers.<sup>99</sup> Fortunately, security experts, and software and hardware developers are moving rapidly to close that technological gap. Their purpose is to make it feasible to establish trust for end-users, be they individual consumers or corporations.

45. Cryptography, the art of spymasters since the time of Julius Caesar, has become an integral part of software development and the act of commercialization of the Internet. I have been asked to share some very basic information about encryption and security that will hopefully demystify the Internet to some extent, and encourage lawyers to counsel their clients to explore ways to capitalize on the public network. Let me crack the code and share some basic tenets of cryptography as it relates to cyber-business. First, where are we on the Internet food chain of security? Security is best handled at two different layers of methodology. One is the network communications layer<sup>100</sup> of the Internet; the other is the applications layer.<sup>101</sup> Second, what is encryption? Encryption is the process of disguising a

---

<sup>96</sup> Gail Bronson is President of InternetAssist.

<sup>97</sup> *See Playboy Enters., Inc. v. Chuckleberry Publ'g, Inc.*, 949 F. Supp. 1032, 1037 (S.D.N.Y. 1996).

<sup>98</sup> *See generally* A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49 (1996) (arguing that unless uncertainties about duties and liabilities are resolved for electronic transactions, growth will be inhibited).

<sup>99</sup> *See* DIGITAL PRIVACY AND SECURITY WORKING GROUP, ELECTRONIC FRONTIER FOUND., PRIVACY, SECURITY, AND THE NATIONAL INFORMATION INFRASTRUCTURE 2 (1993).

<sup>100</sup> The network or communications layer provides a means for entities to route and switch blocks of data through the network and between the open systems in which those entities reside. *See* IBM DICTIONARY, *supra* note 31, at 456.

<sup>101</sup> The applications layer provides a means for application processes residing in open systems to exchange information, and contains the application-oriented protocols by which these processes communicate. *See id.* at 27.

message and scrambling data in such a way that it hides content.<sup>102</sup> The system of cryptography is based on mathematics and it employs algorithms to generate keys. The longer the keys, the more difficult to break into an encrypted message.<sup>103</sup>

46. There are two basic kinds of cryptographic design: symmetric, or secret key cryptography, and asymmetric, or public/private key cryptography. Symmetric key cryptography uses the same key to lock and unlock data.<sup>104</sup> The main drawback is delivering the key to both parties without others finding out. The alternative is asymmetric, or public key cryptography, that employs two key pairs, one public and one private, for each user.<sup>105</sup> The public key is sent to everyone in the system so they can send encrypted data to other people who have the private key to decrypt the message.<sup>106</sup> Encrypting with a private key is equivalent to signing your name because no one else has the same private key. Everyone has your public key, however, so they can identify your signature. The reason public key cryptography has become so wide-spread relative to symmetric cryptography is that it is much easier to manage these public keys. All of this is being done through software applications.

47. There are two commonly used encryption methods today. DES is the data encryption standard globally observed for over 15 years. DES was designed by IBM in the early 1970s and is well established in the financial services world.<sup>107</sup> Another group of computer scientists, Ron Rivest, Adi Shamir, and Leonard Adelman, devised the notion of using prime factorization of integers as part of the RSA cryptosystem.<sup>108</sup> RSA, first presented in 1976 by Whit Duffy and Martin Hellmen, is based on the notion of public-key cryptography.<sup>109</sup>

48. Generally speaking, RSA is better suited for multi-user environments. It does not require the sharing of one secret key. There is a public key and a private key. DES-encrypted communications can only take place among people with prior

---

<sup>102</sup> See Michael Rustad & Lori E. Eisenschmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213, 230 (1995) (explaining encryption).

<sup>103</sup> See Jill M. Ryan, *Freedom to Speak Unintelligibly: The First Amendment Implications of Government-Controlled Encryption*, 4 WM. & MARY BILL OF RTS. J. 1165, 1173 (1996).

<sup>104</sup> See *id.*

<sup>105</sup> See *id.* at 1172.

<sup>106</sup> See *id.*

<sup>107</sup> See Robert L. Hotz, *Computer Code's Security Worries Privacy Watchdogs*, L.A. TIMES, Oct. 4, 1993, at A1.

<sup>108</sup> See Rustad & Eisenschmidt, *supra* note 102, at 231-32.

<sup>109</sup> See *id.* at 231 n. 92.

relationships because they have that same key for encrypting and decrypting.<sup>110</sup> It is wiser to try to use both of them together, which is exactly what financial services and technology titans are working on now.<sup>111</sup> DES is used to conduct fast, bulk encryptions, while RSA allows for secret key exchange between strangers and the creation of digital signatures.<sup>112</sup> Together, they provide the basis of a secure digital envelope for sending encrypted messages across the Internet.

49. Consider the components of developing secured financial service applications on the Internet. A secured transaction of information possesses the following five characteristics: (1) identification of the parties, (2) privacy, (3) authentication, (4) integrity, and (5) non-repudiation.<sup>113</sup> Identification of the parties is the process of verifying the identity of the sender of a message.<sup>114</sup> Since we no longer use sealing wax and signet rings, the identification rests on the notion that some part of the encoded information must positively identify the source. For example, in public key cryptography, digital signatures provide that identification. Privacy is assurance that communications can be conducted without fear of eavesdropping by unauthorized parties. This is, again, achieved through encryption. The ability of cryptography to shield communications is dependent on the key length generated by those algorithms in the encryption system. Authentication is proof of sender and recipient identity.<sup>115</sup> In public key systems, authentication can be achieved through digital signatures. A digital signature is an unforgeable piece of data asserting that the named person wrote or otherwise agreed to the attached message. It is the electronic equivalent of a handwritten signature, only it is created in a software code. Integrity is proof that the transmitted data has been delivered.<sup>116</sup> Integrity of transmitted data is ensured if the data is intact and undamaged, and no one has added or deleted any data from the package during its transmission. Non-repudiation is proof that someone has signed a contract for certain obligations that cannot be denied later.<sup>117</sup> Again, digital signatures are

---

<sup>110</sup> *See id.*

<sup>111</sup> *See id.* at 234.

<sup>112</sup> *See id.* at 232.

<sup>113</sup> *See* Froomkin, *supra* note 98, at 69.

<sup>114</sup> *See id.*

<sup>115</sup> *See* IBM DICTIONARY, *supra* note 31, at 40.

<sup>116</sup> *See* Froomkin, *supra* note 98, at 69.

<sup>117</sup> *See id.*

relevant.

50. As in any industrial revolution, such as the rise of the Internet, whole new industries arise. One cottage industry, that of certification authorities, is arising to assure Internet identities.<sup>118</sup> A certification authority--a third-party company, a bank, an insurance company, or even Coca-Cola on behalf of its employees or customers--will issue certificates that contain the digital identities of those people based on their validation of certain information. For example, a bank might turn over all customer bank card identification information to an outside contractor business,<sup>119</sup> to issue and manage those certificates. Certification information would be very similar to the kind of information you need to get a credit card or a bank card. Banks already have that information, so they would give it to the third party. When individuals conduct business on the Internet, they might be asked to key in their certificates on their computers. Those certificates would reside on the hard drive of their computers, and they would send those certificates off to the server with which they are communicating, whether it is to gain access to their account information at a bank or to complete a shopping transaction.

51. The certificate authorization and distribution business can be very lucrative, especially when it is based on a charge per seat,<sup>120</sup> not unlike an annual fee for a credit card issued by a bank. Recognizing that this could be objectionable, there are other companies that are simply offering to distribute and manage these digital identities.<sup>121</sup> Digital identities must be renewed annually, and certificates must be updated when corporate clients have done the identification checks on their employees or customers themselves. In fact, IBM recently announced such a service in response to requests from their Fortune 500 clients.<sup>122</sup> The idea of a digital identity may sound a little paranoid, but it is very attractive now, especially in the Internet area where employees have to log into multiple databases inside their companies. One digital identity dispenses with the need to use multiple passwords or the same password multiple times. In either case, logging in multiple times is a

---

<sup>118</sup> See *id.* at 55.

<sup>119</sup> See, e.g., Chris Jones, *Banking Spinoff to Issue Digital IDs*, INFO WORLD, Jan. 13, 1997, at 2, available in 1997 WL 8250891 (describing CertCo's introduction of software to distribute risk and liability in electronic transactions).

<sup>120</sup> See Elisabeth Horwitt, *Enterprise Push to Cut Server Costs*, COMPUTER WORLD, May 16, 1994, at 14 (describing seat-based licensing as "paying a set fee based on the total number of workstations").

<sup>121</sup> See *Secure Electronic Transaction Held Up But Verifone Jumps the Gun*, COMPUTERGRAM INT'L, July 15, 1996, available in 1996 WL 10472739.

<sup>122</sup> See *A Closer Look: Commercepoint*, REP. ON IBM (Data Trends Publications, Inc.), Sept. 11, 1996, available in 1996 WL 5803094.

scenario which is much more vulnerable to hacking.<sup>123</sup>

52. Another area of security technology under development and particularly pertinent to the financial services arena is the competition between hardware- and software-based cryptography.<sup>124</sup> As more and more customers move onto the Internet, banks, for example, will be faced with scaling up their hardware to meet heavy usage by customers. This may be problematic. It is simple if there are 5,500 or 1,000 people involved in an electronic system. It is more difficult when there are millions of transactions executed daily.

53. The new protocol for credit card transactions organized by VISA, MasterCard, and many of the Internet technology companies, uses public key cryptography and symmetric algorithms to secure payment information, ensure payment integrity, and authenticate both the merchant and the cardholder.<sup>125</sup> The protocol is the set of instructions everyone will use in developing software so that they can engage in credit card transactions over the Internet.

54. The software implementations of public key cryptography are so computationally intensive, however, that any implementation on a general purpose application server would require more processing time for the cryptography than for accepting and processing the transactions. By analogy, you would be put on hold or somehow backlogged for endless amounts of time, the same way you are put on hold on the telephone. As a result, some technologists have suggested that the superior approach is to move the cryptographic processing off the payment hardware to a special purpose cryptographic device connected as a peripheral.<sup>126</sup> Such equipment should be in the marketplace in the third quarter of this year. For example, one of the vendors, Atalla, a unit of Tandem Computers, Inc., is working with a token maker named VLSI Technology, Inc.<sup>127</sup> to make hardware-based encryption

---

<sup>123</sup> See Camille Mendler, *The Enemy Within*, COMM. WK. INT'L, Nov. 4, 1996, at 260.

<sup>124</sup> See *Internet Commerce Hung Up on Security: Vendors Rush in Where Merchants, Consumers Fear to Tread*, EDI NEWS, Feb. 19, 1996, available in 1996 WL 8070190.

<sup>125</sup> See Rustad & Eisenschmidt, *supra* note 102, at 234.

<sup>126</sup> See *IBM Addresses Online Security With SecureWay*, NEWSBYTES, Oct. 23, 1996, available in 1996 WL 12026176 (describing how IBM has developed technology to plug cryptography co-processors into peripheral component bus slots).

<sup>127</sup> VLSI Technology, Inc. is a company that mass-produces highly customized, highly integrated chips. Their business concentrates on delivering the highest density of customized features on the smallest silicon. For more information on VLSI Technology, see *VLSI* (visited Mar. 24, 1997) <<http://www.vlsi.com>>.

products.<sup>128</sup>

55. Another shortcoming of software cryptographic implementations is their inability to handle encryption services for several applications. Each time a software developer creates an application, he has to license anew and then write in the cryptographic code or the algorithms to his program. As a result, Microsoft<sup>129</sup> developed a universal solution that essentially embeds cryptographic functions into their Windows NT Operating System.<sup>130</sup> The software developer simply calls on the operating system to provide the encryption, signing, or authentication services for the application they are constructing. So companies that create applications for the Web and those conducting banking transactions no longer need to have an in-house cryptographer. They can simply rely on this operating system solution.

56. There are other cryptographic systems. One such system that has just started to gain firepower in the marketplace is called elliptic curve cryptography, first proposed in 1985 by Vic Miller, a research mathematician at IBM.<sup>131</sup> Certicom Corp.<sup>132</sup> of Ontario is the chief purveyor right now, although RSA Data Security<sup>133</sup> and other companies are researching this technology as well.<sup>134</sup> Elliptic curve algorithms are easier to implement and more efficient than other cryptography systems. They are especially well-suited for mobile communications with smaller hardware.<sup>135</sup> For example, Motorola<sup>136</sup> is incorporating elliptic curve cryptography

---

<sup>128</sup> See Jakimar Vijayan, *Making the World a Safer Place*, COMPUTER WORLD, Apr. 15, 1996, at 45.

<sup>129</sup> Microsoft Corp., headed by William Gates, is the world's largest independent software company. For more information on Microsoft, see *Welcome to Microsoft* (visited Mar. 24, 1997) <<http://www.microsoft.com>>.

<sup>130</sup> See *SDI Licenses For Security*, ELECTRONIC COM. NEWS, Sept. 23, 1996, at 1, available in 1996 WL 2329444.

<sup>131</sup> See Paul Barker, *Cashing in on Security*, COMPUTING CAN., Apr. 25, 1996, at 11.

<sup>132</sup> Certicom Corp. is a developer of information security products and cryptographic technologies. For more information on Certicom, see *Welcome* (visited Feb. 20, 1997) <<http://www.certicom.ca/html/main1.htm>>.

<sup>133</sup> RSA Data Security, Inc. provides encryption secured products. For more information, see *RSA Homepage* (visited Feb. 20, 1997) <<http://www.rsa.com/>>.

<sup>134</sup> See *Certicom in Encryption Push*, ELECTRONIC ENGINEERING TIMES, July 29, 1996 at 26, available in LEXIS, News Library, Curnws File.

<sup>135</sup> See *id.*

<sup>136</sup> Motorola, Inc. is an electronics manufacturer and is the world's largest supplier of equipment for cellular telephones, paging and two-way radio. It has formed an alliance with Sun Microsystems to develop products for high-speed Internet access. For more information on Motorola,

into a wireless system that they have been asked to create for Asian countries.<sup>137</sup> Other related Internet technology developments on the horizon are time-stamping<sup>138</sup> and digital watermarks.<sup>139</sup> They will augment the basic cryptographic foundation for providing financial services securely over the Internet.

57. Some argue that securing the public network is dangerous, if not complicated. Is it really worth the effort and the money? All things being equal, the public network is a much more cost-effective distribution channel than the private network or a physical world structure. It is also an attractive alternative for providing access to products and services. The public network is going to be an invaluable convenience in the future. This does not herald the demise of branch-banking or any other kind of branch financial services. It is like television, which did not kill radio. It simply provided an alternative distribution channel with different characteristics that appeal to a certain subset of the audience. If companies can develop secure systems that are marketed appropriately, and they are patient about growing on the Internet in tandem with the rise of Internet usage, then the risk of investment is a no-brainer. But it is not going to be an over-night phenomenon. Export rules, legal liability, digital cash, and policy considerations also need to be addressed. All of these issues converge under the rubric of security and efficiency.

**John Doggett:**<sup>140</sup>

58. Consider the bank vault with its massive walls, and huge steel door with its dials, handle, and tie locks. The vault symbolizes security at the heart of the bank's fiduciary responsibility toward its customers. What are the wheels and mechanisms that are going to secure our financial future in the intangible world? The smart card<sup>141</sup> is the fundamental technology, strengthened by the power of the

---

see *Motorola* (visited Mar. 24, 1997) <<http://www.mot.com>>.

<sup>137</sup> See *Certicom in Encryption Push*, ELECTRONIC ENGINEERING TIMES, July 29, 1996 at 26, available in LEXIS, News Library, Curnws File; see also Mark Moore, *Motorola to Improve the Security of NB-PCS Nets*, PC WK., Sept. 2, 1996, at 40.

<sup>138</sup> A time-stamp indicates the system time at some critical point in the history of the object, such as creation. See IBM DICTIONARY, *supra* note 31, at 694.

<sup>139</sup> Similar to its analog equivalent, a digital watermark identifies the authenticity of an electronic document. See WIRED STYLE: PRINCIPLES OF ENGLISH USAGE IN THE DIGITAL AGE 57 (Constance Hale ed., 1996) [hereinafter WIRED STYLE].

<sup>140</sup> John Doggett is Vice President for Applied Technology at BankBoston.

<sup>141</sup> A smart card is a bank card containing a computer chip for identification, data processing and data storage. THOMAS P. FITCH, DICTIONARY OF BANKING TERMS 571 (1992) [hereinafter DICTIONARY OF BANKING TERMS].



Internet, that will build that foundation of trust, just like that bank vault does. The smart card promises to do the same on the Internet. I am going to make some broad comments, then I will analyze specific, new mechanisms under development to illustrate some of these tools at work, and how they are affecting the security of transactions.

59. One of the key aspects of doing business in electronic form is that you do not know who you are doing business with. Is it an ordinary machine? Is it a person? We do not know. There are some important public cryptography tools being designed to enable you to know with whom you are doing business. The digital signature is a part of that particular methodology.<sup>142</sup> We will utilize digital signature standards set by the government.<sup>143</sup>

60. Authentication is fine, but when we have a transaction passing across the network we want to know that it has certain properties. For example, we may not want it to be read. We may not want someone to tamper with it. I do not want my check or charge card information altered as it moves across the network. Individuals and merchants need to be able to rely on the interplay of the information. Some people may not need privacy all the time, but most people consider financial transactions to be very private and expect them to be protected. So encryption is the tool that can be used for protecting financial transactions. Well-protected, private financial networks are another technique to secure transactions.<sup>144</sup>

61. In the physical payment world, we have many consumer payment mechanisms. You can probably name a half a dozen of them: cash, check, and charge are the first ones that come to mind. Cash, check, and charge mechanisms are being assembled on the Internet right now. The electronic check is an example of a mechanism that requires security. It is interesting that these are following the well-known properties of the kinds of physical exchange media that we have. Cash is anonymous. A check passes from payor to payee, and takes time to navigate the system. Credit card operation on the Internet works in the same fashion. The problems of authentication and the security of transactions are added burdens that have to be addressed in electronic transactions.

62. Consider a real checkbook. The electronic checkbook replaces the paper checkbook; the digital signature replaces the handwritten signature; electronic mail

---

<sup>142</sup> See Henry H. Perrit, Jr., *Legal and Technological Infrastructures for Electronic Payment Systems*, 22 RUTGERS COMPUTER & TECH. L. J. 1, 43 (1996) (stating that by using public key encryption, digital signatures authenticate the identity of a message sender and make forgery impractical and impossible).

<sup>143</sup> See *Approval of Federal Information Processing Standards Publication 186, Digital Signature Standard (DSS)*, 59 Fed. Reg. 26,208 (1994).

<sup>144</sup> See, e.g., Kelly M. Miley, *Electronic Banking*, 15 ANN. REV. BANKING L. 2, 5-6 (1996) (describing alliances between banks and America Online to create secure private networks).

replaces the United States mail; and electronic checks replace paper checks. A payment mechanism for all parties or trading situations is a business in and of itself. Maybe my daughter is at college and I want to send her some funds. It would be easy to e-mail her a check. That is an individual-to-individual transaction. Maybe I received a dividend check by electronic mail so I get a business-to-individual transaction. Basically, electronic checking is designed to handle any of those business situations.

63. With any payment mechanism, we must ensure the security of the mechanism. We must take private keys and ensure that they are private. How can I put them onto my hard drive? It would not take very long before someone cracks my hard drive. What you want to do is authenticate. Authentication would be like your ATM, or automatic teller machine, card that requires a personal identification number ("PIN"). Unfortunately for banks, PINs are becoming archaic. PINs tend to work pretty well at the moment, but in the future they not going to work at all. You want the authenticator on your smart card or electronic card to be held near and dear to your heart. Here, we put the authenticator in the checkbook. We have added some things to the electronic checkbook that you expect to find in a checkbook, like a checkbook register and deposit slips.

64. What are bank certificates? As a receiver of an electronic check, you need to know that documents are authentic. Normally we look at the paper today and it looks good if, for example, it is by the Bank of Boston. But there are some good forgeries as well. We want to prevent forgeries, so we are going to use electronic certificates signed by the bank and some higher authority. We have yet to figure out who is the higher authority. For example, it may be the Federal Reserve. Authentication ensures that the bank-issued card and the account number from which the check will be debited are valid. These certificates form an important part of identification.<sup>145</sup>

65. We need to be able to detect if a check has been altered. I write a check and send it to Nynex. They pay it to their bank. Their bank then moves that check to my bank, where the money is debited from my account and credited to the Nynex account. The electronic check moves in the same fashion initially, and use of this smart card to generate a signature for checks or electronic documents will serve to secure the electronic check. We distinguish between the need for privacy and the need for tamper-proofing. In electronic checks, we protect against tamper-proofing, so that we make the document unalterable or, at least, make alterations detectable.

66. Encryption is usually a function of the link between the payor and the payee. Consider a Nynex bill. Perhaps one does not mind if other people see it. There are, however, certain things that people may not like to have viewed by others.

---

<sup>145</sup> See Froomkin, *supra* note 98, at 58-67 (discussing the function of certificates and the role of certificate issuers).

Encryption can be utilized such that only select individuals can decrypt and read the information using Pretty Good Privacy<sup>146</sup> or one of the other encryption standards. You can authenticate, look at the signature or the bank that issued the bad check. Through the public key system, the payee or the merchant can complete all of those functions. This is completely new. Banks do use signature matches on checks, but signature matching is a very difficult act to perform. The authentication of a check is very difficult, if not impossible, other than by the issuer. Electronics checks, then, can be authenticated by anyone who has the public keys of the issuing party or bank. If used properly, electronic checks are more secure than existing paper checks.

67. As another example, MasterCard and VISA are moving very rapidly towards a smart card implementation of their credit cards.<sup>147</sup> They want to have that authentication in doing their normal transactions because of their significant losses.<sup>148</sup> Encryption is going to be there in the future. This is why it is receiving massive amounts of publicity. There are certainly other types of security, but it is important in the design of systems to continue to improve this kind of security. One goal is to achieve security for consumers and merchants while not making their lives difficult by requiring them to know tremendous keys, all kinds of authentication mechanisms, or tasks that they cannot do. The idea is to maintain a core of convenience and yet have something that is probably secure. This is what designing electronic checks is all about.

68. We divide the world between public access networks and the existing banking systems. These are two mechanisms used in the banking world on a daily basis. The goal is to pass an authenticated message across the line dividing them with no programs, no online working, and no massive computers outside of that line. How do we allow those who are out in the world at large to access these very sensitive internal systems?

69. I have given you a brief look at what is happening in the world of banking, the Internet, and of the security conditions involved in bringing them together. Smart cards are going to be pretty stable and American banks will be using them in

---

<sup>146</sup> Pretty Good Privacy is a free encryption program. See Rich Santalesa, *Feeling Safe and Sound Online; Internet Security*, COMPUTER SHOPPER, Oct. 1995, at 620.

<sup>147</sup> See Jeffrey Kutler, *Smart Cards Gain Two Key Converts: MasterCard, Visa Chiefs Become Big Backers*, AM. BANKER, Oct. 4, 1994, at 1.

<sup>148</sup> See Robert Jennings, *Fraud is Stealing Holiday Joy from Credit Card Companies*, AM. BANKER, Dec. 7, 1995, at 1 (discussing VISA and MasterCard's annual fraud losses of \$645 and \$486 million respectively).

a few years. Smart cards are already in use in France.<sup>149</sup> Smart cards will be an effective device, needed not only in the world of the Internet, but in the physical world as well. As a general application, it is not just the Bank of Boston that is worrying about identifying legitimate customers, but also customers, who worry about whether the Bank of Boston is a legitimate entity on the Internet. How do you know the entity is legitimate? The reason why the French already use smart cards is that they worked for a long time with mere credit cards and suffered massive losses.<sup>150</sup> Hackers were taking secure numbers and account numbers, and while the network was down, they would drain people's accounts from a local bank. This happened in Connecticut.<sup>151</sup> There have been and still are significant problems with banking through the Internet.

**Michael J. Schmelzer:**<sup>152</sup>

70. About 10 months ago, when I was searching for a note topic for my journal, I was looking into the new legal questions around cyber-cash made possible by technology. One of the first things that I found was that the issues raised by the potential anonymity of cyber-cash are not new issues from the banking law perspective. They are old issues. For example, cash transactions over \$10,000 must already be reported.<sup>153</sup> So, although technically it was a fascinating issue, legally it had been done. Today, consider the qualities of money discussed earlier. Consider its anonymity. One of the disadvantages of cash and a trade-off with the benefit of anonymity is that it is inconvenient. It is inconvenient to carry around bundles of bills to do large transactions. This may go by the wayside if an anonymous digital cash system gains acceptance.

71. The government is worried about encryption. They have put export controls on strong cryptography<sup>154</sup> and they have tried to promulgate standards: the

---

<sup>149</sup> See Jeffrey Kutler, *A Smart Card Leader from France Prepares to Mine the U.S. Market*, AM. BANKER, Jan. 19, 1995, at 16; Jeffrey Kutler, *French Banks Try to Sell the U.S. on Smart Cards*, AM. BANKER, Oct. 12, 1993, at 16.

<sup>150</sup> See Kutler, *French Banks Try to Sell the U.S. on Smart Cards*, *supra* note 149, at 16.

<sup>151</sup> See Matt Barthel, *Bank Worker Gets Kudos for Cracking ATM Scam*, AM. BANKER, Oct. 25, 1993, at 24 (reporting that ATM fraud resulted in over \$100,000 in losses to Connecticut banks).

<sup>152</sup> Michael J. Schmelzer was a second-year law student at Boston University School of Law at the time of these comments.

<sup>153</sup> See 18 U.S.C. § 1956(b)(2) (1994).

<sup>154</sup> See 50 U.S.C. §§ 2401-20 (1994).

key escrow standard<sup>155</sup> and the clipper chip.<sup>156</sup> Government officials in favor of the clipper chip want to be able to wiretap terrorists.<sup>157</sup> Their attitude is like an ostrich-head-in-the-sand sort of thing, because terrorists and criminals already have access to strong cryptography, and short of actually outlawing it, there is no way to keep it out of their hands. I call this policy “weak crypto for dumb people.” The second, more legitimate, reason that the government is afraid of cryptography involves money-laundering. Unlike the people who bombed the World Trade Center, when large sums of money are involved, people get smarter and will use better cryptography to cover their tracks.

72. Electronic funds transfers are not new.<sup>158</sup> They have been taking place for over 15 years and the DES encryption standard is what made them possible.<sup>159</sup> But what has changed is that with public key encryption, parties no longer have to communicate over a secure channel.<sup>160</sup> For example, if you wanted to do any off-shore banking, in the past there was a need to go to Nassau or Geneva, open up the account, make the signatures, and verify your identity. With digital verification, you do not actually have to make that suspicious business trip. Moreover, whereas DES encrypted wire transfers between financial institutions were over a secure network where the players knew each other, over the Internet, anyone has access to it and anyone can do it.

73. David Chaum is experimenting with a pay-before system called DigiCash

---

<sup>155</sup> Key escrow refers to the government policy requesting that individuals place their cryptographic private key on file with a trusted third party, but government officials may gain access by filing paperwork showing need for access to the particular key. See WIRED STYLE, *supra* note 139, at 50. The Escrowed Encryption Standard was approved by the Clinton Administration in 1994. See 59 Fed. Reg. 5,997 (1994).

<sup>156</sup> The clipper chip is a national data encryption standard developed by the National Security Agency and proposed by the Clinton Administration to scramble communications, making them unintelligible to all but recipients and government officials. See WIRED STYLE, *supra* note 139, at 17.

<sup>157</sup> See Dorothy E. Denning, *Key Escrow Today*, IBEE COMM. MAG., Sept. 1994, at 58.

<sup>158</sup> See Sarah Jane Hughes, *A Call for International Legal Standards for Emerging Retail Electronic Payment Systems*, 15 ANN. REV. BANKING L. 197, 201-03 (1996) (discussing funds transfer systems, automated clearing houses, securities and commodities markets, and the telex system).

<sup>159</sup> See John Markoff, *Big Brothers and the Computer Age*, N.Y. TIMES, May 6, 1993, at D1.

<sup>160</sup> See Ira S. Rubinstein, *Export Controls on Encryption Software*, in COPING WITH U.S. EXPORT CONTROLS: 1995, at 401, 401-05 (PLI Commercial Law & Practice Course Handbook Series No. 733, 1995).

that guarantees anonymity.<sup>161</sup> We must determine whether or not Swiss banks will use a system like that or whether David Chaum's system will become the equivalent of a Swiss bank. Anonymity is something that could go by the wayside because of abuse. The IRS would probably prefer that all transactions be recorded and traced to reduce the possibility of tax evasion. If we move to electronic funds transfer on the most fundamental level for every transaction, we are not just moving millions of dollars around for buying groceries. We open the door to mandated tracing of every transaction and the concept of anonymous transactions may become a thing of the past.

### Question and Answer Session

*Audience Member:*

74. Do you need a protected communications layer and a protected applications layer, or both? How secure do you need to be?

*Gail Bronson:*

75. Is my wallet secure in my hand; is it more secure in my pocketbook; is it even more secure when my pocketbook is held to my chest? I think that to the extent that government has gotten involved, most business entities have begun to understand that you need both a network layer and an applications layer. The government has moved very rapidly to develop individual types of encryption for the communications layer, the secure sockets layer<sup>162</sup> which is one type of end-to-end solution, and HTTP.<sup>163</sup> Another analogy would be that you can put the money in a Brink's truck and send it down an open highway. If the bandits are around the corner, they will get you. If you just send the money in an open wagon, however, it will not be secure. It is a question of the degree of security, the level of trust that

---

<sup>161</sup> DigiCash was founded in 1990 and offers secure electronic payment systems. For more information on the company, see *DigiCash* (visited Feb. 18, 1997) <<http://www.digicash.com>>. David Chaum patented and markets a system that allows consumers to acquire electronic money with a unique, but anonymous, serial number from a bank. See A. Michael Froomkin, *Regulation of Computing and Information Technology, Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 460 (1996).

<sup>162</sup> Secure sockets layer refers to a Netscape protocol that encrypts data before the user transmits or receives the data. See *Netscape Assistance* (visited Jan. 20, 1997) <<http://home.netscape.com/eng/ssl3/3-SPEC.HTM#2>>.

<sup>163</sup> HTTP, or hyper-text transfer protocol, refers to the original communications protocol of the Web. See WIRED STYLE, *supra* note 139, at 134.

people have in the system, and the amount of security you have to build into the system to imbue the kind of trust that will then engage people to use it.

*John Doggett:*

76. I think security for both the applications and the network layers is required because there are different types of transactions. For example, if you and I are talking on a private channel, a network encryption would be just fine for that kind of application. You are going to get a combination, and then there is always the question of whether or not to put your trust in the network. Whom do you trust? You will tend to want to put your own security where it is warranted. If it is just a chat, we probably would not care. If, on the other hand, we are passing some strategic secret plans, we would probably want to take extra precautions. There will be both kinds of transactions at the end of the day.

77. Consider what happens when a digital signature is out on file. How does a bank authenticate it as it does with the PIN today? The public/private key pair which forms the basis is a linked pair. The private key is not revealed to anyone, yet the public key will be published.<sup>164</sup>

78. There is a mathematical relationship between the two. You know the public key, but you cannot determine the private key. That is one of the properties of public key cryptography. The relationship is proved mathematically.<sup>165</sup> What happens in this case is that you go to your bank with your card and the machine basically computes the public/private key pair. Insert the private key into your card and there would be no record of it.

79. You encrypt the data with your private key. There is another property of public/private key encryption. If I encrypt with my private key, I can only decrypt with the public key; if I encrypt with the public key, you can only decrypt with the private key. This provides a very unique and useful mechanism for passing data and authenticating who signed the document. Therefore, we do not need the signature on file. We need to know your public key. We know it is your public key if you encrypted it and we can decrypt it, and it has your name, address, telephone number, and probably some other identifying information.<sup>166</sup> Then we will know it is from you

---

<sup>164</sup> See W.D. Riley, *Encrypt This!! (E-Mail Encryption)*, DATAMATION, May 1, 1996, at 27, available in 1996 WL 8882494.

<sup>165</sup> Encrypted messages are sent with a code that is the product of two prime numbers. A message sent with the public key (the product) is divided by the private key and the other prime is revealed and used to decode the message. See Thomas Bass, *Whitfield Diffie: A (Semi) Private Conversation with the Headman of the Cypherpunk Revolution (Inventor of Public Key Encryption)*, OMNI, Dec. 1995, at 86, 86.

<sup>166</sup> To confirm the identity of the sender, the receiving party uses the public key to decode the message. See Stewart A. Baker, *The Law of Electronic Commerce*, in DOING BUSINESS ON THE

because that is the mathematical property of public key cryptography.

80. It is this black art of public key cryptography which makes it far more powerful, not only because can we determine that you signed that document, but because anyone in this room that has access to that public key can do the same.

81. In the last two years Bellcore cracked public key cryptography using something like 3,000 computers, six months, and an incredible amount of computing-power.<sup>167</sup> They used brute force. That is, they tried factoring the big number and they tried every possible combination of primes to do that. Consider the key length we are using. We are using 1024 as a key length, so there is a long way to go. This is a two-to-the-power-of-something, an exponent for those of you who are mathematically oriented. That is significantly more difficult to crack than 128. In fact, 129 is being cracked as well.<sup>168</sup> That is a bit worrisome because the technique there was much quicker. This is the worry with public key. Will techniques or computing power move so fast that even 1024 key length is insufficient? The counter argument is that the cryptographers will add more length, going to 2048. They will just keep on going up the curve because there is an infinite supply of numbers.

*Gail Bronson:*

82. There is also the brute force aspect of this. You need a million years of computing power to crack these keys. Stronger and longer keys are being built. How many people are going to get together a million years worth of computing power in one room so that some of the stories related to brute force efforts will be told?

*Michael J. Schmelzer:*

83. One of the things that is accepted as a truism in cryptography is that for a given amount of computing power, it is much easier to encrypt something than to decrypt it. There is an arms race because computers are getting faster and faster, and today's decrypting can decrypt yesterday's encrypting. It is just a matter of keeping pace.

---

INTERNET, at 313, 316-17 (PLI Patents, Copyrights, Trademarks & Literary Property Course Handbook Series No. 452, 1996).

<sup>167</sup> See Loring Wirbel, *Big Bellcore Team Cracks RSA Code*, ELECTRONIC ENGINEERING TIMES, May, 1994, at 1. Bellcore--Bell Communications Research--is a leading provider of communications software and is devoted to developing, improving and expanding technical capabilities to support the telecommunications industry. For more information on Bellcore, see *Welcome to Bellcore*, (visited Mar. 28, 1997) <<http://www.bellcore.com>>.

<sup>168</sup> See Baker, *supra* note 166, at 316.



*Audience Member:*

84. How pervasive will digital cash become in the United States?

*Valerie J. McNevin:*

85. Basically, Hyperion would like to see private money or corporate money. Hyperion wants private money to be issued on the basis of corporate strength. If you look at the different alliances that are occurring around the world, you can begin to see how they are amassing that strength. Look at a copy of the Mondex magazine. It is interesting to look at the advertisements because basically they read, "Whose money is better?" Consider Mondex, DigiCash, and CyberCash.<sup>169</sup> We are moving in that direction. We have a little bit of a problem in the United States because legal tender can only be issued through Congress. Most governments have the same strategy set up in their legal systems, particularly those that have central banks. The United States does not have a central bank.<sup>170</sup> The Federal Reserve does not operate as do the central banks of other countries. A conflict begins when the smart cards and corporate cash identity become stronger in consumers' minds. This is a generational issue. You and I feel very strongly about the greenback that we carry in our wallets, but our children and our grandchildren do not. Mr. Schmelzer's comment about anonymity becoming an irrelevant issue is a comment I take to heart because, for his generation, I think that may well be true. For computer literate teenagers and children, privacy issues are unimportant. Still they are phenomenally significant to my generation.

*John Doggett:*

86. Mondex does not operate in a country without central government approval.<sup>171</sup> In the United Kingdom each Mondex pound has to be reserved with a pound.<sup>172</sup> In other words, that money is effectively taken out of the banking system. What you have is a one-to-one or a fixed exchange rate for these Mondex pounds, giving them the appearance of money. I am not sure whether that fits the concept of private money. With Mondex, the only way you are going to figure out whether

---

<sup>169</sup> CyberCash provides secure Internet financial transaction services. See *News & Info* (visited Feb. 27, 1997) <<http://www.cybercash.com/cybercash/info>>.

<sup>170</sup> Instead the United States is divided up into between 8 and 12 regulatory districts. See 12 U.S.C. § 222 (1994).

<sup>171</sup> See Froomkin, *supra* note 161, at 474-79.

<sup>172</sup> See *id.* at 468-79; see also Lunt, *supra* note 35, at 46.

somebody broke the system is to look at the M1 money supply<sup>173</sup> each month to see if it is unbalanced. If it is heading a certain way, you know someone cracked the code and is manufacturing digital cash. That is a counterfeiting problem on a potentially massive scale. That is a future problem, not one in the current situation where a counterfeiter must get plates and print notes.

*Valerie J. McNevin:*

87. Consider the cultural aspects of electronic money. On Saturdays as a kid in the 1950s, I would go to the bank with a savings book, and put my allowance into my account. I had a relationship with my money, my passbook, and the banker. Today, the bank is full of people on Saturday. They still go in and talk with their banker or with the teller. I have gone to the bank during the week, however, and no one is there. The ATM created a fundamental shift in the way we bank and the role of banks in our cultural consciousness. We no longer use branch banking.<sup>174</sup> From a cultural standpoint, we are stepping away from the trusted institution of the 1950s.

88. Electronic banking greatly affects the branch structure and the trust our generation has in our banks. I just moved from the West to the Northeast. I went through culture shock because I was so used to the ATM. I had not been inside of a bank for many years. When we purchased our home in Connecticut, within two days the mortgage situation was resolved. My in-laws could not comprehend that we did not actually go into a bank, have a long discussion, and establish a significant relationship with our banker before we got a mortgage. There again, you see a generational issue. My in-laws grew up in the Northeast having a very significant relationship with their banker. I grew up primarily in the West having a very significant relationship with my ATM. My debit card is similar. I get to the Northeast and people are still at the grocery store paying cash, but I see my daughter on the computer making purchases. There is a major difference between the way she pursues transactions and the way I pursue transactions.

89. In Canada they have the highest rate of ATMs in the world,<sup>175</sup> and their penetration rate for new technology is significantly higher than that of the United

---

<sup>173</sup> M1 money supply is the basic spendable money supply including currency, demand deposits, travelers checks, and other checkable deposits. See CHRISTOPHER PASS ET AL., THE HARPERCOLLINS DICTIONARY OF ECONOMICS 341 (1988).

<sup>174</sup> A branch is any facility away from the main office of the bank that accepts deposits or makes loans. See DICTIONARY OF BANKING TERMS, *supra* note 141, at 91.

<sup>175</sup> See *Canadians Love Those Debit Cards*, CALGARY HERALD, May 27, 1996, at A3 (noting Canada is one of the heaviest users of credit and debit cards, and automatic bank machines worldwide).

States.<sup>176</sup>

*Gail Bronson:*

90. Consider a third scenario. I just moved from this area back to California. There are plenty of people inside the bank waiting an eternity to go hand over their passbook. There are also plenty of people waiting in line at the ATM. The same thing is true at the grocery store. People think nothing of whipping out a debit card, which is just appalling to me, but you can do it. You can also use your credit card, or good old greenbacks to pay for your groceries. I am the one that said that branch-banking will not be eliminated, and I do not think it will be eliminated. It will just change the choices. Last year a Chicago bank tried to start penalizing people, or charging them, for going into a real branch and talking to people.<sup>177</sup> This was one example of changing choices in banking.

*Audience Member:*

91. What are some current effects of changing technology in the banking industry?

*Valerie J. McNevin:*

92. Let me just tell you about one project that I am working on with an Atlanta bank. We are working on a "virtual bank" for children's use. The children will actually, through virtual reality, go into a bank, into an account, and work with and feel their electronic money. That is just an idea of the future.

*John Doggett:*

93. I was at a retail banking conference two years ago, and the theme of that conference was "The Branch is Dead."<sup>178</sup> I was at the same conference last year and the theme was "The Branch Lives."<sup>179</sup> Let me tell you about Wells Fargo's

---

<sup>176</sup> See John Shoesmith, *Info Highway Now Familiar Road for Most Canadians: Survey*, COMPUTING CAN., May 10, 1995, at 8 (noting that 12% of Canadians have used the Internet).

<sup>177</sup> First Chicago Corp. decided to charge customers \$3 to speak to a human teller. See Timothy L. O'Brien, *Small Accounts Feel Big Squeeze by Big Banks*, WALL ST. J., May 4, 1995, at B1.

<sup>178</sup> See Judge W. Fowler, *The Branch is Dead!*, A.B.A. BANKING J., Apr. 1995, at 40.

<sup>179</sup> See Simon Hally, *Branchless Banking? Don't Hold Your Breath*, CANADIAN BANKER, May 15, 1996, at 1, available in 1996 WL 12008744 (noting that the branch, although changing, survives because the customer still wants face-to-face contact).

experience. They are halving the number of large branches in California but doubling the number of physical customer points of presence.<sup>180</sup> That is, they are actually doubling the branches. What is happening to the branch? The branch is going from a typical 10,000 square-foot, 13-person branch, down to a 50 square-foot branch with an ATM. The nature of the transaction in this new branch is obviously changing.<sup>181</sup> Routine transactions will be automatic and online. In the future, other banking products such as loans, credit, and probably insurance, will be the activities requiring a point of presence or some relationship. Maybe it is not quite as intense as Ms. Bronson and Ms. McNevin are describing here in the East, but there seems to be a West Coast trend of more, not less, branches.

*Valerie J. McNevin:*

94. These new branches are one-person kiosks.<sup>182</sup> To me, the kiosk will eliminate the branch. That is, the kiosk has replaced the branch. The question, though, is whether the kiosk will be recognized and identified as a branch. Consider when you put the bank up on the Internet. Is that a branch site? I think the courts will decide that question in a few years. We have the same question about ATMs. Is an ATM a branch? Does the country, as part of our cultural consciousness, consider an ATM a branch -- a spot in which we put our trust? As we redefine and restructure banking, where does trust fit? Will it be an element of future banking, or will trust be deposited in something else? That goes to the issue of the fiduciary, and how the fiduciary operates in that new construct of a bank.<sup>183</sup> I think it also goes to the concept of Federal Deposit Insurance.<sup>184</sup> How will it relate to the smart card or stored value card? Those are major public policy issues that have to be rapidly addressed.

---

<sup>180</sup> See Peter Sinton, *Wells Plans Expansion in Safeways*, S.F. CHRON., Aug. 2, 1996, at C1.

<sup>181</sup> See *id.* (reporting that mini-branches generate comparable checking and savings account, loan, and investment business).

<sup>182</sup> A "kiosk" has been traditionally defined as a stand or booth at which merchandise is sold or information provided. See WEBSTER'S THIRD NEW INT'L DICTIONARY 1245 (1993).

<sup>183</sup> A fiduciary is a "person or legal entity that administers investments for the benefit of others. A fiduciary is legally obligated to safeguard assets in trust in the best interests of those for whom it acts." DICTIONARY OF BANKING TERMS, *supra* note 141, at 244.

<sup>184</sup> The Federal Deposit Insurance Corporation ("FDIC") insures all deposits of eligible banks and savings associations up to \$100,000. See 12 U.S.C. §§ 1811, 1821(a)(1)(B) (1994).

*John Doggett:*

95. The “new” branch, even if it is a kiosk, has all the functions of a 13-person branch. But it is not a branch. It is a physical point of presence in a business in which tangibility is very important. After a focus group presentation on the image of banks, the participants asked the same question in all the cities, “This is all very good, but where is the nearest branch?” The focus group participants were high-tech people. Yet, they still wanted to know where their branch is because it embodies that trust concept of physical bricks and mortar.<sup>185</sup> With these cards, what is the physical representation of the bank? It is certainly not my personal computer. The card might embody that trust in the future. Ironically, it is going to be a tangible item in this intangible world of the Internet.

96. Banks use the technology when they can. Does the public accept the technology? What is the risk when Bank of Boston sends out the smart card or invites someone to go online with the Internet to do her banking? Is there any personal risk for the customer? Should the people raise these privacy issues with their elected representatives? Is there a threat of a colossal collapse in the monetary system?

97. I guess no warranty is expressed or implied on electronic checks. The laws and regulations we looked at with regard to electronic checks include U.C.C. article 3,<sup>186</sup> U.C.C. article 4,<sup>187</sup> U.C.C. article 4A,<sup>188</sup> among others.<sup>189</sup> These questions always get asked at Internet meetings: “How many of you have done transactions over the network? How many of you have actually used your credit card in an insecure mode?” One or two people out of 100 might raise their hands for the second question. This is typical. The presenter usually challenges them and asks why everybody else is not doing it. Even if someone abuses your credit card number, you

---

<sup>185</sup> *But cf.* Tom Foremski, *Web Browsers Beat Bricks and Mortar*, FIN. TIMES, Sept. 4, 1996, at IT4 (predicting that up to 75% of all U.S. homes will soon use Internet or comparable banking).

<sup>186</sup> *See generally* U.C.C. § 3-104 (defining negotiable instruments); § 3-501(b)(1) (allowing electronic presentment to enforce a negotiable instrument).

<sup>187</sup> *See generally* § 4-110 (authorizing electronic presentment to enforce a negotiable instrument); § 4-209 (retaining an item in furtherance of electronic presentment gives warranty as part of compliance with an electronic presentment agreement).

<sup>188</sup> *See generally* § 4A-103 (including electronic instructions in payment orders); § 4A-201 (defining security procedures for electronic fund transfers); § 4A-202 (defining procedures for authorized and verified payment orders); § 4A-204 (providing procedures for refund for unauthorized payment orders).

<sup>189</sup> *See, e.g.*, 15 U.S.C. § 1693g(a) (1994) (providing for rights, liabilities, and responsibilities of parties in electronic fund transactions).

are liable for \$50, even if the bank enforces the rule.<sup>190</sup> You can basically repudiate that transaction under the current regulations. Yet, only one or two percent of people are engaged in unencrypted transactions on the Internet.<sup>191</sup> This shows that people feel that we need security mechanisms even though the consumer is already very well-protected. In every area of banking law the regulations are tightly written and the oversight is thorough.

98. I do not see any disadvantage in online transactions for the banking consumer. You are essentially governed by the same rules. The Federal Reserve looks at the rules. A great benefit of Regulation E is the printed receipt at an ATM.<sup>192</sup> What if I am on a plane to Chicago with my laptop, dialing into the Internet and I transact business, or I want to take cash out either using my stored value card or by writing a check. Does Regulation E apply? It almost certainly does if I am a consumer, because it is a consumer electronic funds transfer.<sup>193</sup> But what about my printed receipt? Another problem is that the printed receipt has to show location. The regulations are somewhat anachronistic and too specific, but the regulators are changing this. In fact, the regulations are now changed.<sup>194</sup> A new proposal allows a bank to communicate with customers electronically instead of in writing.<sup>195</sup> Within the framework, a tremendous freedom is coming. Nonetheless,

---

<sup>190</sup> See 12 C.F.R. § 205.6 (1996) (providing \$50 consumer liability if consumers notify their financial institutions within two days and increasing liability for later notification).

<sup>191</sup> According to one survey, 22% of online users have purchased goods or services online. Adrienne W. Fawcett, *Online Users go for Facts over Fun*, ADVERTISING AGE, Oct. 14, 1996, at 46. Note that this survey did not distinguish between secured and unsecured transactions, nor between users of online services like CompuServe and users of the Internet. *Id.* However, 45% of users say they are “somewhat or very interested in using online services to make purchases.” Adrienne W. Fawcett, *Interactive Awareness Growing*, ADVERTISING AGE, Oct. 16, 1995, at 20.

<sup>192</sup> 12 C.F.R. § 205.9(a) (1996) (requiring financial institutions to make receipts available for electronic fund transfers at electronic terminals).

<sup>193</sup> An electronic fund transfer is “any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, that is initiated through an electronic terminal, telephone, or computer or magnetic tape for the purpose of ordering, instructing or authorizing a financial institution to debit or credit an account. The term includes but is not limited to, point-of-sale transfers, automated teller machines transfers, direct deposits or withdrawals of funds, and transfers initiated by telephone. It includes all transfers resulting from debit card transactions, including those that do not involve an electronic terminal at the time of the transaction. The term does not include payments made by check, draft, or similar paper instruments at an electronic terminal.” 12 C.F.R. § 205.2(g).

<sup>194</sup> See Electronic Fund Transfers (Regulation E), 61 Fed. Reg. 19,669 (1996).

<sup>195</sup> See Recordkeeping and Confirmation Requirements for Securities Transactions, 61 Fed. Reg. 63,958, 63,963 (1996) (to be codified at 12 C.F.R. § 12.102).

consumer protection is the paramount objective, and I think you are going to have that protection.

99. Consider a consumer who does business with L.L. Bean. The physical presence of L.L. Bean is nothing more than their catalogue. The consumer might not hesitate to give them her credit card number over the phone. She may not stop to think that the person who takes her credit card number over the phone may be also trying to use it personally. She does not stop to think that there might be another person listening to an extension phone at L.L. Bean or, less likely, at her home phone. Experience tells the consumer that most of the time it is perfectly safe.

*Valerie J. McNevin:*

100. I do not agree with Mr. Doggett. I do not believe that the regulations are appropriate yet, and they certainly do not benefit the customer. I feel that a paradigm shift has occurred that is against the public right now, and that is the use of the term consumer. I used to be a bank customer. I prefer to remain a bank customer, not a bank consumer. There is a billboard along Interstate 90, and I do not recall the bank advertised, but the ad reads that if your wallet is empty, you can fuel up at the next ATM. I do not appreciate that advertisement, or the connotations that come with it. Most of the regulators that I work with are very concerned about the lack of customer protection. If you look at a credit report, it says in bold black letters: **YOU ARE RESPONSIBLE FOR YOUR CREDIT REPORT**. The problem is that most customers in this country have no clue as to what goes into that credit report, how it is monitored, how the information in it is accessed, and what they can do about it when something goes wrong.<sup>196</sup> You need to talk to your elected representative, and I think you need to discuss the fact that customers need more education and more protection. Over the last year we have been working with regulators to educate them about this whole process. We do not need to be legislating yet, but we need to educate ourselves so that we can legislate appropriately in the future.

*John Doggett:*

101. I ask the same question. Is the system broken in the area of the credit report? If it is broken, is this because the increasing rate of technology and information is getting out of control? Should there be some slowing, and some tools which will allow for easier clean up of messes? We operate our banking environment within the law and under regulations in the best way to please our customers.

---

<sup>196</sup> See, e.g., H.R. 1015, 103d Cong. (1993) (proposing to amend the Fair Credit Reporting Act to assure completeness and accuracy of consumer information maintained by credit reporting agencies, to better inform consumers of their rights).

Clearly, we want to clean up any mess if it happens. We do the best that we can and try to improve things as time goes by. As a bank gets a reputation for doing that, it attracts more customers.

102. This fundamental problem is best approached within a legal forum because much of it comes back to the law. Congress should address the problem. What things should be done? What kinds of safeguards should be put into place that are not going to increase cost excessively? Usually these laws and regulations increase the cost of doing business.

*Valerie J. McNevin:*

103. In 1993, when terrorists bombed the World Trade Center,<sup>197</sup> many sophisticated companies had backup systems in New Jersey.<sup>198</sup> Then the great unnamed storm of 1993 came through soon after the bombing and wiped out those backup systems.<sup>199</sup> As a result, millions of customers were without ATM service for more than a month in many cases.<sup>200</sup> I could give you other examples of potential problems. We know of several ways of disrupting service through the public switch network and the electromagnetic pulse.<sup>201</sup>

104. There are untested technologies online to decrease the vulnerability of the electromagnetic pulse.<sup>202</sup> Others are still in the minds of the inventors. Typically, most large banking sites have redundancies and backup systems built into their systems. They will have generators and they will have batteries. Still, there are situations where the whole system can crash. The deeper concern is when the jamming of the electromagnetic pulse occurs on just an isolated branch, or a specific kind of transaction, possibly in a hacker situation or a terrorist situation.

105. The jamming can have a phenomenal impact. It is a national security concern.<sup>203</sup> From the United States perspective, it can be a weapon against other

---

<sup>197</sup> See Robert D. McFadden, *Blast Hits Trade Center*, N.Y. TIMES, Feb. 27, 1993, at A1.

<sup>198</sup> See John Holusha, *The Painful Lessons of Disruption*, N.Y. TIMES, Mar. 17, 1993, at D1.

<sup>199</sup> See Robert D. McFadden, *Storm Paralyzes East Coast*, N.Y. TIMES, Mar. 14, 1993, at A1.

<sup>200</sup> See *E.D.S. System is Disrupted*, N.Y. TIMES, Mar. 18, 1993, at D2.

<sup>201</sup> See generally Douglas W. Washington, *Onward Cyber Soldiers: The U.S. May Soon Wage War by Mouse, Keyboard, & Computer Virus*, TIME, Aug. 21, 1995, at 38 (discussing several ways of disrupting electronic communications such as electromagnetic pulse, electronic jamming, and computer viruses).

<sup>202</sup> See *Electromagnetic Pulse Circuit Card Assemblies for the Transportable Single Channel Transponder Receiver Set*, COM. BUS. DAILY, Apr. 15 1996, available in 1996 WL 4975881.

<sup>203</sup> See generally *Hearing on Information Warfare and the Security of the Government's Computer*



countries to bring their economic systems down. The United States is the most vulnerable because we are the most technologically dependent. There are some sites in the country, such as Wall Street and Washington, D.C., where the concentration factor is so large that if you disrupt the magnetic pulse there, you could undo economic systems for a significant period of time.

106. When the disruption is the actual stopping of the signal, it goes on to the timing or the allotment of the disruption. The longer the service is disrupted, the greater the area that is involved in the crashing of the system. There are ways to actually crash the system so that it cannot be revived. You have to simply fix the system and rebuild your records. That potential must be acknowledged so that progress toward recovery mechanisms can occur.