A FIRST STEP TOWARDS CURTAILING ILLICIT CROSS-BORDER I-PHARMA: DRAWING PRACTICAL SOLUTIONS FROM THE REGULATION OF ON-LINE GAMBLING

Karen Eltis*

"I [do not] think the politicians are going to be able to do anything to us.... [It is] kind of like trying to nail Jell-O to a wall."

Bill Reeves of Viapro.com (a cyber pharmacy)

Introduction

The recent death of 57-year-old Marcia Bergeron, which coroners attribute to medication purchased online that was found to contain traces of dangerous minerals (including uranium, strontium, arsenic and lead), revives the debate surrounding rogue cyber pharmacies. Having repeatedly eschewed meaningful regulation, the problem is too often lamentably dismissed as yet another purportedly unmanageable cyber-trend, with fruitful discussion

* Karen Eltis, Associate Professor of Law, The University of Ottawa Law School (Section de droit civil), Law and Technology Research Center member, Ottawa, Ontario.

Acknowledgements: I would like to thank Rony Greemberg for providing the inspiration, tremendous insight, guidance and support, without which this article could not have been written. Thanks also go to my research assistant Mike Henley.

1 The woman, believed to be a U.S. resident, died in British Columbia. See “Coroner blames online pills for B.C. woman’s death” CTV News (21 March 2007), online: CTV.ca <http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20070321/coronер_onolinepills_070321?s_name=&no_adsMar.212007>.

accordingly stifled by an enduring feeling of computer-generated powerlessness.

If nothing else, Ms. Bergeron’s seemingly needless death, apparently as a result of consuming a sedative not legally sold in Canada, underscores the urgency of examining the phenomenon of I-pharma afresh, with an eye towards developing creative responses to cross-border online enforcement obstacles.

It has become no more than a platitude to state that rogue Internet pharmacies – that is to say, those that dole out prescription drugs absent a valid prescription or meaningful physician consultation – significantly imperil consumers. How better to summarize the predicament respecting the regulation of cyber-pharmaceutical crime than with a now infamous incident involving a reporter who obtained Viagra for her cat online, using the animal’s exact height and weight! Tom the cat even received a courteous follow-up e-mail, inquiring into his well-being.

Absent regulation, drugs sold online may of course be counterfeit or untested. They may lack active ingredients or—worse—use toxic excipients. Even when the medication itself is above reproach, the lack of meaningful physi-

---


4 See Joe Wilcox, “Drugstores get a check-up in Congress” CNET News (30 July 1999), online: cnet news
   <http://news.com.com/2100-1017-229270.html>: In Kalamazoo, Michigan, TV station WWMT-News 3 launched an investigation of online pharmacies, and was able to order ten 100 mg tablets of Viagra for a patient named Tom. The only problem: Tom was a house cat. In the online questionnaire, the station indicated that Tom stood 6 inches tall, weighed 15 pounds, and was neutered. WWMT also received Viagra for a reporter’s dead grandfather and for a station employee who reported that he had heart trouble and took nitrate medicines. Viagra is potentially fatal when taken in combination with nitrates.

See e.g. Sean P. Haney, “Pharmaceutical dispensing in the ‘wild west’: advancing health care and protecting consumers through the regulation of online pharmacies” (2000) 42 Wm. & Mary L. Rev. 575 at 590.

cian oversight or (more alarmingly perhaps) the illusion thereof is decried by professional associations as endangering patients’ health and very lives.\(^6\)

Whereas legitimate online pharmacies – as distinguished from their rogue counterparts – \(^7\) are usually associated with traditional pharmacies and require consumers to provide a valid prescription before any drugs are expedited,\(^8\) the questionable (or “quasi-rogue”) sites discussed herein instead allow patients to simply fill out a questionnaire, which is followed by a “diagnosis” and prescription from a virtual doctor.

Notwithstanding the pretense of diagnosis, this format is tantamount to self-medication since the i-doctor routinely rubber stamps the patient’s exact specifications.\(^9\) The above reference to the feline being prescribed erectile dysfunction medication leaves little doubt as to the propriety of this approach if left unchecked.

It is worth noting that aside from aiding individual patients to avoid the awkwardness of discussing conditions such as those referenced above, these sites are also sought out by those with criminal intent, seeking drugs such as Rohypnol and other medications associated with date rape and sequestration.

Worse yet, purely rogue Internet pharmacies, for their part, make no pretense of even requiring diagnosis or prescription, simply permitting consumers to freely purchase the drugs of their choice, including controlled sub-

---


\(^7\) See discussion of types of e-pharmacies in Part I below.

\(^8\) Some of these sites operating in Canada sell into the U.S. As a matter of general interest, the Canadian Patented Medicines Prices Review Board (PMPRB) regulates pricing on pharmaceuticals, which are therefore less expensive in this country. For a more extensive discussion see Simon R. Rabinovitch, “On the Legitimacy of Cross-Border Pharmacy” (2005) 43 Alta. L. Rev. 327.

\(^9\) See discussion of types of e-pharmacies in Part I below.
stances. These latter sites, described and differentiated below, specifically form the object of this present inquiry.

In addition to safety concerns, the sale of counterfeit medication and improper storage of drugs of lesser quality occasion millions in lost pharmaceutical revenues, thus depriving researchers of precious funds and further raising the soaring price of medication. This in turn, paradoxically, compels consumers to seek refuge from these unaffordable prices on-line, effectively perpetuating a vicious cycle.

With regard to privacy – which sometimes prompts consumers to seek out I-pharma ab initio, ironically – these fly-by-night e-pharmacies (which the Washington Post labeled “pipeline[s] for narcotics” are known to sell or misuse confidential patient information, and regularly flood Web surfers with unwelcome spam.

11 Both rogue and “quasi-rogue.”
12 The WHO estimated that, in the 1990s, 10% of the world’s branded pharmaceuticals were counterfeit, with that number rising to 50% in developing nations. “Spot examinations of foreign drugs shipped to the United States by the Food and Drug Administration (FDA) and the United States Customs Department revealed that 88% of such drugs were unapproved by the FDA or counterfeit.” See Linda C. Fentiman, “Internet Pharmacies and the Need for a New Federalism: Protecting Consumers While Increasing Access to Prescription Drugs” (2003) 56 Rutgers L. Rev. 119 at 129.
14 See Nicole A. Rothstein, “Protecting Privacy and Enabling Pharmaceutical Sales on the Internet: A Comparative Analysis of the United States and Canada” (2001) 53 Fed. Comm. L.J. 343 at 346, n. 8: “From a privacy protection standpoint, the architectural structure of the Internet itself presents concerns because it is a global ‘network of computer networks,’ and digital information often passes through dozens of computers before reaching its intended destination. Thus, an individual’s health care information shared over the Internet is potentially more vulnerable to unauthorized access.”
15 Ibid.
Not only missed work days, out of pocket expenses\textsuperscript{16} and cost of care (particularly for the uninsured in the U.S.),\textsuperscript{17} but privacy concerns, then, impel the urgency of effective regulation.

From a Canadian perspective specifically, it would be sorrowfully misleading to dismiss the matter of uncontrolled cross-border i-pharma – as some may be tempted to do – as being offset by its purported revenue-generating potential for local pharmacies. Instead, not only do rogue i-pharma products endanger patient safety – a matter of concern to all governments – but for Canadians, they present the additional challenge of potentially compromising our entire price-regulated system,\textsuperscript{18} arguably jeopardizing billions of dollars in research and development. In a word, therefore, controlling improper I-pharma engages the values of both safety – reducing preventable injury or deaths – and accessibility to affordable drugs.

It is important to note that prior attempts at setting parameters across borders, both normative and extralegal, have met with consistent failure. Thus, for instance, “Operation Cyber Chase,” a year-long initiative that targeted “international Internet pharmaceutical traffickers operating in the

\begin{itemize}
\item \textsuperscript{16} \textit{Supra} note 12 at 124, n. 16. As Fentiman points out, “During the anthrax scare of 2001, Internet pharmacies played a significant role in the skyrocketing sales of Cipro.”
\item \textsuperscript{18} As the Canadian government explicitly regulates prices of patented drugs, unlike its US counterpart. While it is beyond the scope of this piece to delve further into this complex and important issue, suffice it to note that the proposed regulation targets rogue I-pharma sites, the majority of which are foreign and by no means benefit legitimate Canadian pharmacies, with which they unfairly compete. Instead they compromise safety and accessibility. Indeed: “There are concerns on both sides of the border about online pharmacies. Some question the ethics of Canadian doctors who are willing to write prescriptions for U.S. patients they’ve never examined. Meanwhile, others are concerned Canadians could face supply shortages, lower quality service and risk losing federally regulated prices as pharmacists try to cater to the U.S. market.” See “Cross-border Rx” \textit{CBCnews} (17 January 2006), online: cbc.ca <http://www.cbc.ca/news/background/drugs/>.
\end{itemize}
United States, India, Asia, Europe and the Caribbean,”\textsuperscript{19} was, like many others, unsuccessful.\textsuperscript{20}

Not surprisingly, effective regulation of cyber-phama crime is highly complex, raising intricate issues of jurisdiction, in addition to those pertaining to criminal law, intellectual property, and consumer protection and competition law \textit{inter alia}. Not only do attempts at cross-jurisdictional regulation, referred to above, generally fail, they result ironically in a proliferation of harms as more sites move out of the regulating country – further complicating matters jurisdictionally.\textsuperscript{21}

While by no means indifferent to the relevant complexities, the primary aim of this paper is to propose an approach that – although both preliminary and indirect in nature – arguably holds significant promise of mitigating, if not curtailing, some of the severe harms associated with questionable and rogue cyber-pharmacies.

The remedy in question is inspired by recent efforts to control a similarly compelling challenge: on-line gambling.

By seeking to bypass some of the painstaking issues surrounding online policing – particularly of the cross-border ilk – this proposal serves as a necessary \textit{first step} in a process that quite bluntly appears paralyzed. Accordingly, part of the contribution’s significance lies – if nowhere else – in its ability to

\textsuperscript{19} The purpose of this operation was to crack down on “rogue” Internet pharmacies that distribute Schedule II through Schedule V controlled substances – such as narcotics, amphetamines, and anabolic steroids – to consumers without a prescription issuing from a physician, as required by the law of the United States. See U.S. Drug Enforcement Administration, News Release, 202-307-7977, “International Internet Drug Ring Shattered” (20 April 2005), online: U.S. Drug Enforcement Administration <http://www.usdoj.gov/dea/pubs/pressrel/pr042005.html>. See also John Richard Castronova, “Operation Cyber Chase and Other Agency Efforts to Control Internet Drug Trafficking: the ‘Virtual’ Enforcement Initiative is Virtually Useless” (2006) 27 J. Legal Med. 207.

\textsuperscript{20} It is beyond the scope of this paper to discuss the numerous failed and unsuccessfully attempted initiatives in any detail. Suffice it to remark that traditional state and federal police actions targeting rogue Internet pharmacies are futile as use of the Internet, lack of state and federal resources, and location in foreign nations make it difficult to locate and prosecute rogue Internet pharmacies.

alleviate the paralysis that plagues law and policy making respecting Internet regulation.

The following therefore consists of a preliminary proposal for regulating the unlawful cross-border sale of cyber-pharmaceuticals, derived by analogy from comparative inquiry. Significantly, the proposal outlined below is preemptive rather than responsive in its prescriptions and is, in this manner, distinguishable from previous attempts.

To satisfy this paper’s prescriptive objective, it will first be necessary to preface the regulation of I-pharma analysis with a discussion of the phenomenon itself, however succinct. In so doing, the paper adopts the following structure:

Part I provides an overview of the various types of Internet pharmacies (or I-pharma) and the concerns and challenges that they respectively raise. Faithful to the comparative method, but by no means exhaustive in scope, Part II proceeds to a brief and rudimentary survey of the relevant regulatory framework in both the US and Canada, highlighting the particular difficulties pertaining to cross-jurisdictional sites. The aim again is to offer an overview rather than a thorough analysis of the legal framework, leading into Part III, which most importantly perhaps sets forth the proposal forming the subject of this writing, derived from the regulation of I-gambling.

**Part I: Types of On-Line Pharmacies: An Overview**

As previously noted, not all online pharmacies are created equal, and their distinct incarnations are most pertinent to this inquiry. For present purposes, let us divide I-pharma into three categories: the conventional, the quasi-rogue, and rogue cyber drug providers.

**A. Conventional I-Pharma**

The first category that I made reference to above might best be labeled the “conventional” I-pharma or what Fentiman deems “the Internet versions of a ‘bricks and mortar’ pharmacy.”22 These are commonly extensions of physi-

22 *Supra* note 12 at 126, n. 23: “Some of these Internet pharmacies have been specifically endorsed by the National Association of Boards of Pharmacy (NABP) as meeting appropriate standards of pharmacist licensure, quality
cal pharmacies, created for consumer convenience, and require patrons to provide a valid prescription from an accredited physician, as they would in the physical world.\textsuperscript{23}

Some of these sites are not without controversy in the U.S., primarily with regard to Canadian or other foreign entities reaching into that market with far cheaper product.\textsuperscript{24} As noted, however, the issue of patent protection – essential to research, development and innovation, as highlighted above – is of great relevance on this side of the border as well.

This facet, however important,\textsuperscript{25} is beyond the scope of this discussion.\textsuperscript{26}

Instead, as previously noted, the following opts to focus exclusively on addressing the two other types of cyber-pharmacies. Labeled quasi rogue and rogue respectively, these pose dangers to: consumer safety, research and development, and access to affordable medications.

In this vein, an elucidating survey by the National Center on Addiction and Substance Abuse (CASA) reveals that:


\textsuperscript{23} As Nicolas P. Terry explains: “these legal Internet-based pharmacies are distinguishable by reference to their business model; they do not offer prescribing services but fill prescriptions that, while frequently electronically transmitted, are written by a traditional healthcare provider.” See Nicolas P. Terry, “Prescriptions sans Frontieres (or How I Stopped Worrying about Viagra on the Web but Grew Concerned About the Future of Healthcare Delivery)” (2004) 4 Yale Journal of Health Policy Law and Ethics 183 at 188, 223.

\textsuperscript{24} Supra note 8 at 332.

\textsuperscript{25} Or with respect to generic drugs that are introduced therein while the original US patent is still active.

\textsuperscript{26} For a more thorough discussion of the cross-border pharmacy sale of prescription drugs to U.S. patients by Canadian I-pharma and the controversies generated thereby, see supra note 8.
Of the 157 sites selling controlled prescription drugs on the Internet:

- 90% did not require prescription
- 41% stated that no prescription was needed
- 49% offered an “online consultation.”

Herein lays the importance of distinguishing these illicit incarnations from their conventional counterparts.

B. Quasi-Rogue Sites

Sites that this author refers to as “quasi-rogue” are those in which a patient – having signed a waiver of liability and selected a drug of choice – is asked to complete a medical questionnaire, which is then forwarded to an online doctor for “diagnosis.” Based on this questionnaire – and, ostensibly, the consumer’s self-diagnosis and specifications – the latter prescribes medication, most often conforming to the patient’s particular drug preference.

Arguably, these sites raise greater concerns than their purely “rogue” counterparts (discussed below), if only by reason of their prim appearance and trappings of legitimacy (i.e., a “consultation” and “prescription” by a “virtual physician” to go with your desired order of medication). Consumers are thereby lulled into a false sense of safety.

Although documentation is scarce, the understanding seems to be that virtual physicians merely rubber stamp orders, prompting the American Medical Association (AMA) to vociferously decry and condemn these sites. Accordingly, in 2003, the AMA Board of Trustees issued a statement warning:


29 Supra note 14 at 347: “The majority of medical experts agree that the Internet today offers a hodgepodge of useless and misleading information mixed in with very relevant and reliable medical information.”
An online questionnaire (or online consultation) with no interpersonal interaction is insufficient....[A] physician may increase his or her liability exposure by prescribing medications to individuals solely through an online interaction. Moreover, such physicians put themselves at increased risk of disciplinary action by their state boards of medicine.  

Furthermore, cyber-pharmacies of this ilk tend to misrepresent themselves as originating from jurisdictions perceived as “trustworthy,” i.e. developed countries such as Canada.

The reality, however, is quite different, as these statistics indicate:

- A study performed by Cyveillance for the FDA found that of 11,000 sites it found claiming to be Canadian pharmacy websites, only 1,009 actually sold prescription drug products, and of those, only 214 were registered to a Canadian entity. The remaining 795 pharmacy sites had registration information indicating a US

30 American Medical Association Board of Trustees, *Report of the Board of Trustees: Guidance for Physicians on Internet Prescribing*, online: American Medical Association <www.ama-assn.org/ama1/upload/mm/annual03/bof7a03.rtf> [AMA, Guidance for Physicians]. The Special Committee on Professional Conduct and Ethics of the Federation of State Medical Boards of the United States requires prescribing physicians meet four requirements:

1) an adequate patient evaluation, including the taking of a medical history and a physical examination;
2) an exchange between the patient and physician sufficient to identify the risks and benefits of alternative treatment approaches;
3) a subsequent treatment review to assess its therapeutic outcome; and
4) [the] maintenance of a contemporaneous medical record...readily available to patients and their other health care professionals.


31 A study of 11,000 Internet sites that were designed to look like Canadian pharmacies revealed that only 214 were actually registered in Canada. See Robyn Lamb, “Study finds many online discount pharmacies are misrepresenting themselves” *The Daily Record* (14 June 2005). See also *supra* note 14.
owner (the majority) as well as owners in Vietnam, the Czech Republic, and Barbados.32

- Of those, only 1009 sold prescription medications, and only 214 were actually registered in Canada; 87 were registered in Barbados. Other companies were registered in Vietnam, Germany, Australia, El Salvador and Mexico.33

Their purposefully deceptive character, fraught with misrepresentations respecting both the product dispensed and its very origin – in addition to the chimera of physician oversight they create – speaks to the danger these sites pose.34

C. Rogue I-Pharmacies

Finally, mention has been made of rogue Internet pharmacies which, for their part, allow customers to freely purchase the medication of their choosing as they would apparel or cosmetics – without prescription and absent medical oversight. It is as simple as that: “Point, Click, Self-Medicate.”35

Evidently, these raise a panoply of concerns, as a recent UN report (International Narcotics Control Board)36 underscores:

a) Pharmaceutical products sold may be marketed using inaccurate assertions at best, fraudulent ones at worse. Thus, for instance, websites commonly advertise that their drugs come from Canada when in fact “they frequently came from Malaysia, Vanuatu or Eastern Europe.” Rates of counterfeiting in such places are high,

32 AMA, Guidance for Physicians, supra note 30.
33 Ibid.
35 Review of Consumer Safeguards, supra note 22.
but that aside, the likelihood of drugs being time-expired or incorrectly stored are extremely high.\textsuperscript{37}

b) The products in question – issued without a prescription or absent the supervision of a physician or pharmacist – are likely ill-suited and can therefore present severe health risks.\textsuperscript{38} As Clifton rightly observes: “consumers who try to self-diagnose may be unaware of the possible side effects of certain medications. Those consumers also risk an adverse reaction with other prescriptions they may already be taking.”\textsuperscript{39}

(To illustrate the point dramatically yet again,\textsuperscript{40} an American news station obtained Viagra for two pets, a deceased person, and a man with cardiac disease).\textsuperscript{41}

c) The product could easily be counterfeit or expired. Counterfeit drugs are easy to produce, are financially lucrative, and pose a low risk to the seller. Indeed, “A fake pill may cost less than $0.01 to make, but can be sold for $0.30, and that is still cheaper than the actual drug. In addition, the risk and cost of selling licit drugs is much lower than that for illicit drugs.”\textsuperscript{42} As Brian Liang points out in his instructive article:

\textsuperscript{37} See “Top European Security Expert Warns Senate Panel on Risk of Drug Importation” \textit{PharmaLive} (19 April 2005), online: PharmaLive <www.pharmalive.com>. In a similar vein, Terry warns: “Even though the domain names for these businesses may ‘look’ American (i.e., dot. com), it is likely that a large percentage are based offshore.” \textit{Supra} note 23 at 189.

\textsuperscript{38} See e.g. Kara M. Friedman, “Internet Prescribing Limitations and Alternatives” (2001) 10 Annals Health L. 139 at 145-46 (noting that the risks include “potentially harmful side effects from inappropriately prescribed medications, dangerous drug interactions, and delay in seeking necessary medical intervention”).

\textsuperscript{39} \textit{Supra} note 28 at 546; see also Yoo, \textit{supra} note 10.

\textsuperscript{40} See Wilcox, \textit{supra} note 4.

\textsuperscript{41} See generally Haney, \textit{supra} note 4.

Rogue Internet and mail order pharmacies are seen to be the primary source of counterfeit drugs within the next five years...The WHO and the FDA estimate that annual worldwide sales of counterfeit drugs are between $32 billion and $35 billion. The FDA warns that this financially lucrative counterfeit drug trade is linked to funding terrorist activities.\(^43\)

Anecdotal evidence too abounds. Thus, for instance, NBC Dateline investigative journalist Chris Hansen posed as a company representative seeking out Internet suppliers of counterfeit medicines. Within weeks, he received multiple offers from all over the world for a variety of drugs – including counterfeit Viagra and Tamiflu.\(^44\)

One provider has already been convicted of selling counterfeit HIV testing home kits.\(^45\)

In such cases, as Liang explains:

Harm occurs in at least three ways. First, if the fake drug contains the wrong drug, the patient is not treated for the disease he or she has...Wrong or ineffective drugs not only fail to help the patient get better but also contribute to the increase in antibiotic resistance of bacterial pathogens, making infections harder to fight...The third common method of harm results when the fake drug has no active ingredients and indeed may have harmful ingredients added to make the drug more realistic. In these circumstances, patients are not only harmed by not being treated, they are sometimes killed by materials used to make the fake drug. Counterfeiters have introduced bacteria-laced water...colored dye, powdered cement, toxic

\(^{43}\) Ibid. at 285.

\(^{44}\) See Chris Hansen, “Traveling through the world of fake drugs” Dateline (2 June 2006), online: MSNBC <http://www.msnbc.msn.com/id/13099555/#060609a>. According to Hansen: “The supply line took us all the way to Hong Kong, where in a modern hotel room outfitted with hidden cameras, we met with a woman who told us she was a major player in this illicit business. Even we were surprised when the woman, who called herself Cherry Wong, agreed to ship us thousands of fake Viagra tablets a week, a deal that could be worth $10 million.”

yellow road paint, floor wax, boric acid (the latter used commonly to kill cockroaches), and, horrifyingly, antifreeze....

d) The price paid could be higher than in legal pharmacies. These sites play outside the regulated market – exempt from transaction costs – and can offer their products at much lower prices. That in turn paradoxically raises the price of licit medication, thereby prompting consumers to turn to their illicit counterparts out of financial need.

e) The purchaser’s personal information – such as name, address, credit card and medical information – may be compromised.

f) Concern is exacerbated in the case of seniors, who form a significant percentage of prescription drug users.

• Greater than 80% of seniors use at least one drug, 50% report taking at least three prescription drugs ... Although seniors account for only 13% of the population, as patients they account for more than one third of all prescriptions, and as payers they account for more than 40% of each dollar spent on drugs each

---

46 Supra note 42 at 283-84.

One of the most insidious means of selling counterfeits is salting. Salting occurs when legitimate drugs or fakes with some active ingredient – which are often imported from other countries or have expired – are mixed or “salted” with fake versions of the drug. In this way, even if patients, pharmacists, or government authorities are attempting to detect counterfeits, these fake drugs may elude detection due to a legitimate sample or fake with the active molecule being pulled for testing.

Supra note 42 at 285 [footnotes omitted].

47 Supra note 36 at 4.

48 Supra note 14 at 368. See also Kerry Toth Rost, “Policing the ‘Wild West’ World of Internet Pharmacies” (2000-2001) 76 Chicago-Kent L. Rev. 1333 at 1342: “Some drugstores sell confidential patient information to third parties conducting marketing campaigns for drug manufacturers. This inappropriate or inadvertent disclosure of private medical or prescription information can lead to a variety of problems, such as employment discrimination, increased health or life insurance premiums, and even denial of insurance coverage.”
year. It is estimated that seniors alone spent more than $70 billion on prescription medicines in 2005.\(^{49}\)

This with more and more seniors surfing the net due to limited mobility and isolation.

**Part II: Attempts at Regulation in Canada and the U.S.: A Comparative Apercu**

Having outlined the issues, let us proceed with a concise synopsis of the relevant regulatory framework currently in place in the United States and Canada. At this juncture, it is crucial to note that the *éventail* of potentially applicable norms is most vast and eschews a proper presentation in this context. Therefore, as noted, the following refrains from detailing the black letter normative framework, a task proficiently tackled by many a scholarly writing elsewhere.\(^{50}\) Instead, it will be content to flag the issues, sparing any in-depth examination.

**A. The United States**

In the United States, online pharmacies are subject to both state and federal law, which provides for a significant measure of self-regulation by relevant professional bodies.

---

\(^{49}\) Supra note 42 at 280.

(i) The Federal Level

Broadly speaking, the Federal Government oversees drug safety and importation. This momentous enterprise involves multiple federal statutes and several empowered agencies.\(^{51}\)

Most prominent amongst these are: the FDA, deriving its mandate from the Federal Food, Drugs, and Cosmetic Act;\(^{52}\) the FTC, authorized by the Federal Trade Commission Act to “protect consumers from unfair or deceptive acts or practices;”\(^{53}\) and the Drug Enforcement Administration (DEA), created by the Controlled Substances Act of 1970.\(^{54,55}\)

*Inter alia*, the Federal Food Drugs and Cosmetic Act requires that prescription drugs be procured only with a valid prescription *and* under a physician’s supervision. It likewise prohibits the re-importation of drugs manufactured in the U.S. and the importation of prescription drugs lacking FDA approval.\(^{56}\)

And yet, by patronizing an offshore Internet pharmacy website, American consumers can easily obtain drugs without a prescription or consultation – even medications not approved by the FDA.\(^{57}\)

In an ironic twist, William Hubbard, Associate Commissioner for Policy and Planning at the FDA, himself observed that the “FDA has no ability to

---

51 For a more complete discussion see Ayres, *ibid*.
52 9 U.S.C. 21 §§ 351, 352(a)-(c), (e)(1), (e)(3), (e)(4), (f)-(j), (n)-(r), and 355(a)(1)-(4), (b)-(d), (e), (j)(4) (2000) [FFDCA].
55 See *supra* note 42.
56 *Supra* note 52 § 381.
57 This notwithstanding the fact that, as Liang observes: “According to the FDA: virtually all prescription drugs imported for personal use into the United States ... violate the [Federal Food, Drug, and Cosmetics Act (FFDCA)] because they are either unapproved new drugs (21 U.S.C. § 355), labeled incorrectly (21 U.S.C. §§ 352, 353), or dispensed without a valid prescription (21 U.S.C. § 353(b)(1)).” See *supra* note 42 at 284. Importing a drug into the United States that is unapproved and/or does not comply with the labeling requirements in the FFDCA is prohibited under 21 U.S.C. §§ 331(d) and/or (a). *Ibid*. § 381(a).
take effective action against these foreign operators on behalf of US citizens.”\(^{58}\) A fortiori, the same is true for the FTC and DEA.

In addition, federal laws criminalizing wire fraud and mail fraud can be relevant in instances involving consumer fraud via the telecommunications or postal system. Accordingly:

these federal laws can be used when deception, fraud, and unlawful practices are identified on websites. Since it is difficult to recognize these rogue sites and to regulate their actions... agencies within the Department of Justice, such as the FBI and the DEA, often work with other state and federal agencies in locating fraudulent and illegal online pharmacies and bringing these violators to justice.\(^ {59}\)

The above-mentioned DEA, for its part, “is responsible for enforcing federal drug laws and is also involved in the regulation of pharmaceutical drugs over the Internet. Federal laws in this vein apply if a pharmaceutical company attempts to dispense a controlled substance over the Internet.”\(^ {60}\) For our purposes, the DEA – not unlike the FDA – “maintains that the Internet has not altered federal drug laws and that all controlled substances must, therefore, ‘continue to be dispensed pursuant to a valid prescription, obtained from a legitimate physician-patient encounter.’”\(^ {61}\)

It bears repeating that despite various attempts at monitoring and enforcement by each of these agencies, successful regulation – particularly with regard to foreign based I-pharma – remains elusive.\(^ {62}\) This by reason of both geographic and related jurisdictional issues, the broad yet intricate scope of which, as noted, far exceeds this discussion.\(^ {63}\)

\(^{58}\) Liang, \textit{ibid.} at 310.

\(^{59}\) \textit{Supra} note 6 at 964-65.

\(^{60}\) \textit{Ibid.} at 964.

\(^{61}\) \textit{Supra} note 18 at 143.

\(^{62}\) Indeed, “Internet dispensing is increasingly an international phenomenon involving many regulatory actors and a complex legal landscape.” See \textit{supra} note 23 at 203

\(^{63}\) See e.g. Michael A. Geist, \textit{Internet Law in Canada} (North York: Captus Press, 2000) at 41 ff: “As Internet law has developed, a two-step analytical approach has emerged. First, court, regulators and legal practitioners must determine what law applies... [a]ssuming the applicable law can be identified, the analysis then shifts to a second step consisting of determining who is entitled to apply the law.”
Plainly put, “overseas pharmacies do not come within the jurisdiction of the United States.” What is more, as the U.S. General Accounting Office’s (GAO) study reveals, I-pharma sites are dispersed worldwide, which makes them even more difficult to track down (hence the jello reference above). Thus, for instance, the GAO counted 21 foreign sites located in countries ranging from Argentina, Costa Rica, Fiji, India, Mexico, Pakistan, the Philippines, Spain, Thailand, and Turkey – all 21 of which either featured an e-questionnaire or had no prescription requirement at all.

Consequently, as has been repeatedly commented, the sale of drugs through foreign websites creates a compelling challenge for US law enforcement and the difficulty – both legal and political – regarding asserting jurisdiction over these entities cannot be overstated.

64 Yoo, _supra_ note 10. For a discussion of jurisdictional issues, regarding both offshore entities and difficulties arising between US states, see Reidenberg, _supra_ note 50. See also _supra_ note 6 at 972.


66 “The sale of drugs to U.S. residents via foreign websites is an extremely challenging area .... Foreign sales pose the most difficult challenge for U.S. law enforcement because the seller is not within U.S. boundaries. Although the FDA may have jurisdiction over a resident in a foreign country who sells in violation of the [Food, Drug and Cosmetic Act] to a U.S. resident, from a practical standpoint, the Agency working with DOJ has a difficult time in enforcing the law against foreign sellers, when they are hard to reach and outside our borders.” See William K. Hubbard, “Statement of William K. Hubbard Associate Commissioner For Policy and Planning Before the Committee on Government Reform U.S. House of Representatives Hearing on Internet Drug Sales March 18, 2004,” online: U.S. Food and Drug Administration <http://www.fda.gov/ola/2004/Internetdrugs0318.html>.

**ii) The State Level**

Not surprisingly, these constraints are *a fortiori* true with respect to regulation and enforcement at the state level.

Briefly, states have traditionally regulated health insurance, prescription dispensing and health care providers themselves.™ They license and discipline physicians and enforce general consumer protection norms.

In their efforts to fulfill this important mandate, most states deem the physician-patient relationship a prerequisite to a legal drug sale™ (involving, at a minimum, a face-to-face meeting before prescription drugs can be legally dispensed™) and have legislated accordingly.

Thus, for instance, over forty states have passed laws requiring “out-of-state pharmacies, including online pharmacies, to receive a permit from the State Board of Pharmacy.”™

Illinois, New Hampshire, and New York, for example, require that all online pharmacies that dispense medications to their residents: first, be licensed in some American state; second, disclose all relevant licensing information – as well as the identity and addresses of corporate officers – on their

---

68 See *Dent v. Virginia*, 129 U.S. 114 at 122 (1889) (upholding 93 Act W. Va. §§ 9, 15 (1882)): “The power of the State to provide for the general welfare of its people authorizes it to prescribe all such regulations as, in its judgment, will secure or tend to secure them against the consequences of ignorance and incapacity as well as of deception and fraud...The nature and extent of the qualifications required must depend primarily upon the judgment of the State as to their necessity.”

69 Federation of State Medical Boards of the United States, *Model Guidelines for the Appropriate Use of the Internet in Medical Practice* (Dallas: Federation of State Medical Boards of the United States, 2002), online: Federation of State Medical Boards of the United States <http://www.fsmb.org> [FSMB].

70 For a more in depth discussion see Hochberg, *supra* note 50. See also Clevenger, *supra* note 50 at 179-80.

71 See *supra* note 12 at 151.

websites; third, maintain adequate records of drugs dispensed; and fourth, provide a minimum of forty hours a week of toll-free telephone service to consumers.  

Maine, New Hampshire, and Vermont, for their part, ask that “any medical service to a patient requires a professional licensor in the state in which the patient encounter will occur” [emphasis added]. As is the case more often than not, lack of uniformity amongst states prevails. Some states use existing frameworks while others have enacted specific statutes.

A California statute, as a final illustration, provides that “[p]rescribing, dispensing, or furnishing dangerous drugs ... without a good faith prior examination and medical indication therefor, constitutes unprofessional conduct.” Indeed, “California remains the only state with a full-time agent dedicated to investigating online pharmacies.” Therefore, California “permanently revoked the license of a California physician who had written more than 11,000 prescriptions for patients via the Internet without ever examining them.”

Of course, such measures can only prove effective in the local (as distinguished from the offshore) context, when the offending physician or entity has some tie to the state.

Needless to say, that is also true for other relevant legal remedies (not discussed here) – criminal law, tort law and consumer protection laws,

73 Ibid. at 150.
74 Ibid.
76 Supra note 28 at 552.
77 Supra note 12 at 149.
79 Counterfeit drugs or drugs containing dangerous excipients that cause death or injury to consumers could expose the provider to a slew of criminal charges at both the federal and state level. Broad categories (at the Federal and State level, respectively) include but are not limited to:
- Conspiracy to commit health care fraud
- Conspiracy to distribute controlled substances
- Sale of pharmaceuticals on the Internet without valid prescription.
80 Tort (civil liability) has been an area of law touted as boding promise in tackling
for example. Here, too, success can only be achieved locally, if at all, for obvious reasons.

Finally, there is professional self-regulation.

In that vein, the American Medical Association explained that Internet prescribing falls well below the minimum standard of medical care for the following reasons:

1. There is no examination of the patient to determine if there is a medical problem and to determine a specific diagnosis;
2. There is no dialogue with the patient to discuss treatment alternatives and to determine the best course of treatment;
3. There is no attempt to establish a reliable medical history;
4. There is no provision of information about the benefits and risks of the prescribed medication; and
5. There is no follow-up to assess the therapeutic outcome.

I-pharma. Therefore, “some states have initiated civil actions against pharmacies that fill prescriptions without a physical examination of the patient.” Typically, however, states have “attained only modest civil penalties, restitution.” See Andrew Somora, “Direct-to-Consumer Advertising: Are Consumers Being Informed?” (1998-1999) 8:2 Kan. J. L. & Pub. Pol’y 205 at 206. The problem, as some have argued, may be cultural, deriving from “lowered expectations of the doctor-patient relationship, pharmaceutical companies have increased direct-to-consumer advertising, thereby in the patient’s eyes reducing the need for a physician to be involved in determining what drug therapy to use.” See supra note 28 at 548.

Privacy laws may also be of relevance in terms of information misuse or even identity theft. When ordering through quasi rogue or rogue sites, customers are providing name, address, credit card information and health information. This information is often misused or resold to entities that may misuse the information, potentially resulting in harassment or spam (at best) and identity theft (at worse). While privacy law does come into play, unfortunately, as discussed elsewhere, the normative framework relevant to privacy is far from generous – particularly in the US.

For a summary of personal jurisdiction difficulties in the Internet context generally (as well as a host of law enforcement problems) see Reidenberg, supra note 50 See also Eric M. Peterson, “Doctoring Prescriptions: Federal Barriers to Combating Prescription Drug Fraud Against On-Line Pharmacies in Washington” (2000) 75 Wash. L. Rev. 1331 at 1332-34.

See AMA, Guidance for Physicians, supra note 30.
Although of undoubted pertinence conceptually, all this – as previously discussed – matters little in the cross-border context since most rogue and quasi-rogue Internet pharma sites originate offshore and function outside the effective control of any state\(^{84}\) or federal government,\(^{85}\) let alone professional associations.

Not surprisingly, this conundrum is no less true north of the U.S. border, as the following overview reveals.

**B. Canada: Relevant Legal Framework**

The normative framework can best be described as sparse. Whereas prescription drugs are regulated primarily at the federal level,\(^{86}\) the provinces administer health care, including the licensing of health care providers and the managing of medication programs.

More specifically:

federal regulations dictate that prescription drugs may be dispensed by a Canadian pharmacist only by order of a ‘practitioner,’ defined as ‘a person authorized by the law of a province of Canada to treat patients.’ Provincial legislation in Ontario and Quebec narrows prescribing authority further, requiring that the physician be licensed in the pharmacist’s province; conventional pharmacies across Canada tend to follow this practice even in the absence of a legislative requirement to do so.\(^{87}\)

In theory at least, dispensing prescription pharmaceuticals over the Internet is therefore presumably only lawful if the cyber pharmacy is of the above described traditional ilk – in other words, connected to a bricks-and-mortar pharmacy – thus ostensibly precluding rogue or quasi-rogue Canadian sites.\(^{88}\)

---


85 For a discussion of cross-border jurisdictional issues see Reidenberg, *supra* note 50.

86 *Supra* note 14 at 371.

87 See *supra* note 8 at 347-48.

Cross-border pharmacies are of course subject to the same licensing requirements as conventional brick-and-mortar pharmacies. In Ontario, for example, Internet operations have been investigated by the College of Pharmacy for alleged violations of licensing requirements under the *Regulated Health Professions Act, 1991*[^89] and the *Drug and Pharmacies Regulation Act*.[^90]

Finally, like in the US, self-regulation is also prominent, by various provincial pharmaceutical associations and physician colleges.[^91] But again, professional bodies are left as impotent as their governmental counterparts in this realm for reasons discussed above.

What then can be done?

**Part III: Seeking Solutions: Applying Lessons from the Regulation of Online Gaming to I-Pharma**

In an effort to address the above-stated difficulties, Part III comprises two related prongs: *First*, it offers a brief discussion of Title VIII of the recently passed *Security and Accountability for Every Port Act of 2006*[^92] (hereinafter: the “Act”), and of the New York settlement that seemingly inspired it. I refer here to the *Spitzer Initiative* that served to secure the consent of several important financial institutions and payment facilitators to disallow online gaming transactions.

It next shows that *certain* edifying lessons might be drawn from indirect methods focused on internet intermediaries[^93] and applied to cutting off payment sources for cross-border pharmaceutical misfeasance.[^94]

More specifically, this paper’s primary objective is to submit that the focus on Internet *intermediaries* – particularly e-payment facilitators – in com-

[^91]: The scope of which is beyond our objective.
[^93]: Be it “voluntary” (i.e., by securing the cooperation of financial institutions, credit card companies and other e-payment facilitators, a la Spitzer) or by legislation similar to the Act – in spirit if not logistics.
bating illicit borderless online activity (be it by securing “voluntary” consent, as in the Spitzer initiative, or via explicit legislation, as per the Act) heralds a noteworthy advance in cyberlaw enforcement – one that lends itself particularly well to I-pharma regulation. What is more, while this model has met with legitimate criticism in the gambling context from whence it originates, I argue that those critiques lose a great deal of their potency with respect to cyber-medication due to important distinctions between these respective milieus (i.e. healthcare versus gambling).

For as discussed below, unlike gaming, which presents value-laden issues of personal autonomy versus state coercion and Constitutional constraints in the U.S., cyber-pharmaceutical consumers do not – for the most part – deliberately aim to purchase harmful (perhaps even deadly) medication, or to eschew the law. Instead, by and large, they visit these sites for convenience (not covertness), openly seeking out what they believe to be lawful or at least safe prescription medication, rather than counterfeit or expired products.

What is more, in contradistinction to what are generally sophisticated gamers, often-times actively attempting to evade normative constraints in their online activities, most I-pharma consumers are trusting law-abiding individuals – many of them seniors – seeking the law’s protection in avoiding questionable sites harmful to their health, rather than looking to circumvent the law clandestinely.

With that in mind, and prior to further dwelling on the distinctions between gambling and pharma/health, it appears useful to broach both Title VIII of the Act and the Spitzer Initiative that preceded it, with an eye towards distilling valuable lessons applicable to curtailing cyber pharmaceutical crime.

No thorough discussion of the Act or the regulations applicable thereto is offered; instead, what follows is (like Part II) a succinct overview.

---

95 Relating primarily to freedom of expression as government – some might say paternalistically – endeavors to constrain the practice of a certain activity or lifestyle against its citizens’ expressed will.

96 Needless to say, those who are not (such as the above mentioned sexual offenders seeking to purchase Rohypnol and the like) are far from making a “life style” choice, as gamblers argue on their own behalf.

97 See Gottfried, supra note 94.
A. Targeting I-Gambling Intermediaries: An Introduction to the Act

In the United States, gambling was traditionally the province of state regulation. In contradistinction, Internet gambling incrementally devolved to – or, according to some, was usurped by – Federal authorities. Not unlike most cross-border cyber quandaries, attempts at controlling cyber gambling met with modest success (at best) and generated little beyond frustration (at worse).

Then in 2006, Congress passed the Security and Accountability For Every Port Act of 2006, a piece of legislation that at first glance has little to do with cyber gambling. Rather, its stated purpose is to enhance the security of United States ports on the heels of mounting preoccupations in that vein. A closer look, however, reveals an interesting addition thereto: Title VIII of the Act. Named the Unlawful Internet Gambling Enforcement Act of 2006, Title VIII governs online gambling.

In an effort to prevent U.S. residents from gambling at offshore Internet casinos, this Title specifically prohibits the transfer of funds from a financial institution to an I-gambling website.

98 See Raj, supra note 94. Under the Interstate Horseracing Act, 57 U.S.C 15 § 3001 (2000), Congress specifically found that gambling is the primary responsibility of the States (“The Congress finds that ... the States should have the primary responsibility of determining what forms of gambling may legally take place within their borders”).


100 See generally Reidenberg, supra note 50.
101 Supra note 92.
103 The FBI and the Department of Justice argue that Internet gambling serves as a medium for money laundering activities, potentially exploited by terrorist organizations.
104 Subject to certain exceptions, including some online lotteries, horse/harness racing and fantasy sports.
Following this general guiding principle, regulations are to be drafted in order to “add details and specificity to the Act by providing financial institutions with specific policies and procedures to follow.”

For our purposes, Title VIII’s significance resides not in measuring the success it has ostensibly achieved to date in the gaming context (such analysis is arguably premature and better performed elsewhere), but with its underlying philosophy: that of targeting intermediaries – credit card companies and other financial institutions that make virtual payment possible – rather than undertaking to regulate questionable offshore I-sites per se.

The rationale behind this paper’s full attention towards applicability to I-pharma can therefore be summarized thusly: since offshore Internet gambling is funded primarily through credit cards and wire transfers, the idea is to target – and ideally desiccate – the transfer of funds to sites deemed unlawful. Accordingly, “the law prohibits any person from accepting money from someone who has engaged in unlawful Internet gambling.” It bears repeating: the idea is chiefly to dry up funding, so to speak, thereby attacking the phenomenon of elusive cross-border sites indirectly.

Since offshore entities (in this case casinos) themselves evade effective regulation – for reasons discussed at length elsewhere – it is preferable that policy makers turn their attention towards well-established intermediaries with domestic roots that enable the impugned transactions via their financial services. In other words, financial intermediaries, primarily credit card issuers with significant local assets – rather than the gambling sites themselves – form the object of regulation under this model.

Since issuers are in a position to identify Internet gambling activity by the use of transaction codes, they are held to recognize suspect codes and to be able to deny proscribed transactions, irrespective of geographic origin.

The advantage, quite obviously, is that the issuers are generally local (or boast some significant financial ties to the United States), thereby providing incentive to comply with US (or Canadian) law and presenting none of the

---

105 See Raj, supra note 94 at 789 and at 808: “The recent Unlawful Internet Gambling Enforcement Act is focused on solving these problems. The Act itself does not provide a solution, but does authorize the Board of Governors of the Federal Reserve System to promulgate regulations that can solve these enforcement problems.”

106 Rather than the black letter normative framework itself.

107 See Raj, supra note 94 at 789.

108 Ibid.
pitfalls ordinarily associated with cross border cyber regulation of elusive foreign entities. Plainly put, the principle underlying the Act, as it respects online gambling, is one of indirect regulation aimed at curtailing the financial transactions associated with the illegal activity, given the inadequacy of direct enforcement of gambling laws.\footnote{Ibid. at 806: “Before the passage of the Unlawful Internet Gambling Enforcement Act, the enforcement of an online gambling prohibition in the United States was extremely weak.”} One can see the applicability of this approach to the realm of cyber pharmaceuticals.


In addition, financial intermediaries need not be “targeted” or directly regulated. Instead their participation may be voluntarily secured. Indeed, the thinking leading up to this model of indirect cross-border cyber-enforcement may well have been sparked by a settlement spearheaded by then New York Attorney General Elliott Spitzer. The 2002 agreement involved major credit card companies (led by Citibank) and Pay Pal consenting to bring to an end the use of their payment methods for Internet gambling transactions.

One is not at all surprised to discover that an unenforceable court victory (in the New York case of *People v. World Interactive Gaming*, in which the state succeeded in obtaining a conviction against an offshore Internet casino despite its tenuous connections to New York\footnote{See *People ex. Re. Vacco v. World Interactive Gaming Corp.*, 714 N.Y.S.2d 844 at 848-50 (Sup. Ct. 1999) (holding that defendants, an offshore company offering Internet gambling to New York residents, were subject to personal jurisdiction in New York).}) led to a shift in thinking, with law enforcement innovatively choosing to curb Internet gambling by focusing on the payment system instead of the casinos sites themselves.

In view of that, New York’s Attorney General obtained Citibank’s and other important financial institutions’\footnote{New York Attorney General Eliot Spitzer has signed agreements with 10 banks to block cardholders from using their credit cards for transactions identified as online gambling. See supra note 110.} agreement to block offshore gambling transactions in the following manner: “The credit card transactions are ‘coded’ by merchants and their merchant banks to indicate to credit card...
issuing banks (the lenders) what is being purchased. By blocking certain of these codes, issuing banks can avoid extending credit for much gambling activity that occurs on the Internet.”

As noted, PayPal, the leading e-payment facilitator, also agreed to stop online casinos from using its facilities to take money from New York gamblers.

This indirect regulatory tactic, focusing on established payment facilitators rather than elusive offshore merchants (i.e. casinos) themselves proved quite effective as a means of overcoming cross-border cyber jurisdictional obstacles that the law has yet to address.

In effect, while certainly not foolproof, “all online gambling sites listed on the London Stock Exchange or similar markets have stopped taking United States players due to the passage of the Act, while most non-public companies have announced an intention to continue taking US customers.”

113 Ibid.


115 See Jack Goldsmith & Timothy Wu, “National boundaries have survived in the virtual world – and allowed national laws to exert control over the Internet” Legal Affairs (January-February 2006), online: <http://www.legalaffairs.org/issues/January-February-2006/feature_goldsmith_janfeb06.msp>. According to Goldsmith and Wu: “…the technique seemed to work pretty well, driving half of Antiguan web gambling firms out of business, and, in the words of the Antiguan prime minister, leaving a ‘significant, negative impact upon the [Antiguan] economy.”’ Nevertheless, trade issues arise. Thus, for instance, in the latest action in a World Trade Organization dispute between Antigua and the United States, the WTO ruled on January 25, 2007 that the U.S. is in violation of its treaty obligations by not granting full market access to online gambling companies based in Antigua. See Declan McCullagh, “WTO slams U.S. Net-gambling ban” CNET News (7 April 2005), online: CNET <http://news.cnet.com/WTO-slams-U.S.-Net-gambling-ban/2100-1030_3-5658636.html>. See also Mike Brunker, “Will ban end Internet gambling? Don’t bet on it” MSNBC (17 October 2006), online: msnbc <http://www.msnbc.msn.com/id/15240569/>.

C. Applying the Gaming Approach of Targeting Internet Intermediaries to Cross Border I-Pharma

(i) The Critique: A Word

This model, although innovative and readily applicable to curtailing the illicit sale of I-pharma, is – as may be expected – far from flawless. In effect, it has met with criticism on three levels in the gambling context: first, respecting the First Amendment issues that it potentially raises relating to gamers’ freedom of expression; second, respecting its effectiveness – particularly the ability of Internet gambling providers to deliberately camouflage their transaction codes to avoid detection and denial of proscribed transactions; and third, respecting the shifting of the cost and burden of enforcement onto financial institutions.

(ii) Distinction between I-gambling and I-pharma

The criticisms directed at the Act – particularly the third prong relating to cost – certainly have their place and merit. Although a proper appraisal of the censure leveled in the gaming arena far exceeds the scope of this endeavor, the following remarks nevertheless bear mentioning.

For our purposes, a fundamental distinction – already alluded to above – must be drawn between Internet gambling and the sale of cyber-pharmaceuticals. These differences render the application of the aforementioned model particularly apt in the pharma context (even more so than with re-


119 See Brunker, *supra* note 115: “The biggest obstacle to an effective federal ban is the Automated Clearing House network, or ACH, an electronic processing system used by the Federal Reserve that currently can’t tell a gambling transaction from a mortgage payment.”

garding to gambling) and give good reason for entertaining its use in curtailing the sale of dangerous cross border i-medications in an effort to protect patient health and safety.

Protecting consumers from expired, counterfeit or otherwise hazardous medications that the great majority of I-pharma purchasers would presumably wish to avoid rather than seek (since we are dealing with websites purporting to sell otherwise legal medications, not illegal substances) conforms to government’s mandate of safeguarding basic public safety – not the imposition of moral choices (games of chance). As for controlled substances, obtaining any prescription medications – let alone controlled substances – without a prescription is otherwise illegal. Why should it be any different online? This falls within the ambit of the state’s traditional regulatory role, not within the ambit of autonomy and life-style choices.

The next challenge, of course, will be to identify which sites might bear the dubious distinction of being “unsafe” (rogue or quasi-rogue) and to ensure that financial institutions are given the proper incentives to cooperate, rather than are unilaterally constrained to support associated burdens.

Let it be emphasized: suggesting the intermediary model as we do is but a first step. Presumably, follow-up would involve international cooperation at some level and a recognized international body (such as UNESCO) would probably be best qualified to issue licenses or VPN numbers to legitimate sites that have passed certain health and safety tests, in a manner similar to FDA or Health Canada approval (since the sites are not limited to one particular jurisdiction).

Another possibility, the fleshing out of which exceeds the purpose of this present endeavor, is one offered by the Royal Pharmaceutical Society of Great Britain, which has developed a pilot project giving persons placing orders through Internet pharmacies direct access to its website to enable them to verify whether an Internet pharmacy is duly registered with the Society.

As to effective regulation – or perhaps more accurately enforcement – the focus has been on how easily creative gamblers can avoid control by resorting to forms of payment that cannot distinguish between barred transactions and lawful ones.121 As already observed, unlike gamblers, prescription drug

121 See Brunker, supra note 115:
The biggest obstacle to an effective federal ban is the Automated Clearing House network, or ACH, an electronic processing system used by the Federal Reserve that currently can’t tell a gambling transaction from a
purchasers – particularly those most vulnerable, such as the elderly, who form a significant proportion of I-pharma consumers – are not generally sophisticated or seasoned shoppers and, in contradistinction to gamblers, they generally use traditional credit cards (rather than resorting to covert purchase methods designed to avoid traceability). That in itself is arguably a much-needed start.

The idea that not all crime can be successfully intercepted remains, of course, as true here as it is elsewhere in the penal realm. It is a necessary beginning.

**Conclusion**

The preceding sets forth the model to be followed at the level of principle. The logistics, it is submitted, should be fleshed out by policy makers so as to comport with these recommendations. Clearly, decisions by relevant stakeholders will have to be made as to whether the “voluntary” or normative approach is preferable in this context. That having been said, the idea of indirect online enforcement through the regulation of jurisdictionally established financial intermediaries can spark a transformation in our normative thinking in this context.

The above-described proposal’s novelty, coupled with the now infamous attacks leveled at it in the gambling context, surely render a sober assessment of its success in that vein rather premature.

---

122 For example, enlisting private sector intermediaries speaks to the general difficulty relating to co-opting the private sector to do government bidding in the Internet context. This raises important privacy and other problems that must be addressed. For a fuller discussion generally see Ian R. Kerr, Alana Maurushat & Christian S. Tacit, “Technical Protection Measures: Tilting at Copyright’s Windmill” (2002 - 2003) 34 Ottawa L. Rev. 7.

123 Not surprisingly, the American gaming lobby has rallied against the legislation, which various legislators have threatened to repeal. Thus, in April 2007, U.S. Congressman Barney Frank introduced a bill overturning the gambling aspects of the Act, saying “The existing legislation is inappropriate interference on the personal freedom of Americans and this interference should be undone.” See Barney Frank, News Release, “Frank Introduces Internet Gambling Regulation
That said, the Act – not unlike the Spitzer initiative – constitutes, if nothing else, an inventive response to what once presented itself as yet another insurmountable cyber-quandary. Accordingly, and for that reason alone, it impels sustained exploration respecting its application in the I-pharma context.

This arresting simple scheme is of surprising utility for addressing cross-border Internet problems, particularly cyber pharmaceuticals. It is by no means a panacea but a much welcome initial step towards enforcement.

As the above has aimed to submit, the focus on financial intermediaries, as distinguished from direct regulation, holds significant promise for the regulation of transnational cyber crime and related issues.

Like their I-gambling counterparts, Internet pharma sites are in many instances outside the reach of U.S. or Canadian jurisdiction. Some cyber-pharmacies are fly-by-night entities, able to skillfully skirt effective regulation. It is for this very reason that the indirect model that aims to cut off payment to such sites rather than to shut them down – although admittedly imperfect – presents important promise for curtailing the sale of health-hazardous cyber-pharmaceuticals and for promoting patient safety.

Indeed, as discussed in the preceding section, there is the fact that seniors are particularly vulnerable to the dangers inherent in illicit cyber-pharma-


125 Patient deaths are of particular concern. As the paper’s opening story starkly illustrates, “Canada has not been immune to counterfeits and deaths associated with such drugs; coroners, the Royal Canadian Mounted Police, and the Ontario College of Pharmacists are currently investigating several deaths associated with imported counterfeit cardiac drugs sold from a pharmacy there and have brought charges against another pharmacist for selling fake drugs.” See supra note 42 at 296-97.
ceuticals. In light of obvious mobility constraints and a documented preference for net surfing,\footnote{126} the elderly especially value the convenience of online medication, as do many others in this increasingly Web-dependant age.

The cross-border trade of rogue i-pharma is a complex phenomenon, rendered more intricate by changes to technology occurring on an almost daily basis. What is apparent is that the current “do nothing” approach is economically costly in terms of development and innovation, severely compromises patient safety and – paradoxically – endangers Canadians’ access to affordable drugs by ultimately dragging down Canada’s regulated system.

Faced with this reality, carefully applying certain aspects of the gaming framework to I-pharma, prohibiting banks and credit card companies from accepting payment for rogue\footnote{127} i-pharmacies, may be an idea whose time has come.


127 Please see above for a discussion of definitional criteria for what constitutes a “rogue” I-pharmacy. The discussion is meant to offer some preliminary guidance and is by no means exhaustive. An important challenge for implementing a proposal such as this will of course be for policy makers to flesh out such criteria carefully and soberly – the logistics of which would necessarily constitute the next step in the regulatory process.}