Chapter 3
Internet Pharmacy Cybercrime:
State Policy Mitigating Risks 2000–2015

Mary Schmeida
Kent State University, USA

Ramona S. McNeal
University of Northern Iowa, USA

ABSTRACT

Internet pharmacy social gains are efficiency, improving pharmaceutical access for isolates, and less cost. Alongside gains, illegal Internet pharmacies and unscrupulous pharmacy practices have made online purchasing a cyber risk for consumers. Industry self-regulation has failed, giving way to U.S. government and transnational intervention. The U.S. assumes “responsible domestic governance” in disrupting Internet crime by passing modern day drug policies (White House, 2011; 2016), and having transnational cooperation. States have joined the federal to pass laws generally on licensed in-state entities processing orders for rogue Internet pharmacies (GAO, 2013) but not uniformly. However, online pharmacy sites continue to dispense without “valid” prescriptions, unapproved drugs are sold online, and illegal pharmacies continue to operate. This chapter explores why some American states have adopted laws regulating Internet pharmacies from 2000 through 2015, using Cox proportional hazards regression.

DOI: 10.4018/978-1-5225-1941-6.ch003

Copyright ©2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
INTRODUCTION

Internet pharmacy improves access to medications for geographically remote populations and those seeking to pay less, but with risks. As Internet accessibility grew and the e-pharmacy industry moved global, transnational e-pharmacy cybercrime becoming more evident. Government response has been piecemeal, with federal regulations improving consumer safety, administrative laws, and U.S. transnational cooperation. Domestic governance requires the states to enact legislation mitigating cybercrime (White House, 2011, p.11). Since states do not have jurisdiction over international pharmaceutical markets, and in fiscal stress, it has been difficult to disrupt illegal Internet pharmacies. Generally, states have focused their oversight on licensed in-state entities processing orders for rogue Internet pharmacies (GAO, 2013). Not all states are mitigating risks uniformly as state legislative action varies significantly.

In this chapter, we explore why some American states 2000-2015 have passed laws regulating risky Internet pharmacy activity, whereas other states remain laggard. It also discusses the policy context, players, and policies. Policy implementation theory suggests a number of factors may impact the extent to which state action is taken in passing laws, factors such as political constraints and state resources. The impact of these factors on policy adoption is explored using Cox proportional hazards regression.

BACKGROUND

Considered e-commerce or digital trade, e-pharmaceutical growth in the U.S. has been rapid with online pharmacies having the highest profile of e-health business for consumer trading, as seen with pharmaceutical and beauty aid sales for 2012 valued at 14.68 billion U.S. dollars (Statista, 2015). However, illegal Internet drug outlets (National Association of Boards of Pharmacy [NABP], April 2015) and unscrupulous pharmacy practices (Schmeida, 2005) have threatened the safety of online medication purchases (Schmeida & McNeal, 2015). Nearly 11,000 websites sold medications to U.S. consumers illegally from 2008 to 2014 (NAPB, January 2015, p.3) most transnational in operation, selling drugs that are counterfeit, substandard, and without a valid prescription (GAO, February 2014). Counterfeit meds lead “patient safety threats perpetuated by rogue websites” (NABP, April 2014, p.7). According to the INTERPOL report of June 18, 2015, 156 worldwide arrests were made of transnational criminal networks selling counterfeit medications through illicit Internet pharmacies (p.1).
Are Online Privacy Policies Readable?
www.igi-global.com/article/online-privacy-policies-readable/43058?camid=4v1a

A New SOA Security Model to Protect Against Web Competitive Intelligence Attacks by Software Agents
www.igi-global.com/chapter/new-soa-security-model-protect/49510?camid=4v1a