Contracting for Privacy Precaution (and a Laffer Curve for Crime)

Ian Ayres

ABSTRACT

While Internet consumers and retailers have incentives to contract to protect against criminal privacy invasions by third parties, externality and observability concerns may limit contractual precaution mandates. Contracting between consumers and retailers operates, however, in the shadow of government efforts to deter cybercrime—which in turn can influence the equilibrium information-sharing activity levels as well as private precaution efforts taken by consumers and retailers. This article argues that there is a criminal analog to the Laffer curve. Just as citizens' reaction to taxation policy raises the possibility that, over some range, lower tax rates may produce higher government revenues, citizens' reaction to penal policies raises the possibility that, over some range, higher penalties may produce more crime. Though victims and thieves may be made better off by a "higher crime–higher penalty" equilibrium, these private benefits must be measured against (among other things) the social costs of additional state effort.

1. INTRODUCTION

While many articles in this issue discuss the efficiency of contracts authorizing retailers to use consumers' data, another important use of contracts involves precautionary promises by both consumers and retailers to prevent unauthorized third parties from obtaining and using this information. This type of unauthorized theft of information is an important species of cybercrime.

When a third party hacks into a user's account and not only gains access to the user's personal data such as passwords and profile information but also gains the ability to direct purchases to the hacker's own benefit, the user loses autonomy and self-authorship. Identity theft is not just a species of privacy invasion; it is a violation that is often much worse than

IAN AYRES is the William K. Townsend Professor at Yale Law School. Omri Ben-Shahar, Rick Brooks, Anthony Cozart, and Lior Strahilevitz provided helpful comments.

[*Journal of Legal Studies*, vol. 45 (June 2016)]
 0047-2530/2016/4502-0021$10.00

the misappropriation concerns that arise when retailers repurpose consumers' information without sufficient consent. And unlike retailer misappropriation, third-party misappropriation often results in financial as well as autonomy-related costs. Lifelock earns more than $400 million annually for a service that purports to reduce the likelihood of identity theft. But there is no Lifelock for privacy—that is, no comparably successful service to protect against improvident retailer misappropriation of users' information.

This article explores how contracting between consumers and retailers affects precaution taking and how this interacts with government policies to influence the prevalence of cybercrime. In particular, it is posited that higher penalties may (counterintuitively) produce more crime and that both consumers and retailers may benefit from this relatively greater prevalence. This benefit, however, must be measured against the costs of implementing and enforcing additional penalties. This argument is organized into two parts: the first part discusses the precaution-taking incentives and provisions in consumer-seller contracts and the possibility that externality and observability constraints will produce suboptimal precaution levels. The second part explores how this equilibrium between consumers' and retailers' behaviors is likely to be influenced by different levels of government precaution taking and whether different policies could nudge precaution-taking behavior in desired directions.

2. PRECAUTION TAKING ARISING FROM THE CONSUMER-RETAILER CONTRACT

Contracts between Internet consumers and retailers can reduce the likelihood of cybercrime by mandating that both consumers and retailers take precautions to prevent it. For example, when a website requires that a user register with a password that is at least eight characters and contains at least one uppercase letter, one lowercase letter, and one number, the seller is requiring, as a prerequisite to contracting, that the consumer engage in precaution taking that exceeds the level that the consumer would otherwise have chosen. These precaution mandates alter consumers' behavior. There is strong empirical evidence that a substantial number of users, left to their own devices, would choose extremely weak passwords. Users often use identical passwords across multiple accounts (Ives, Walsh, and Schneider 2004; Bang et al. 2012). In addition, passwords are frequently based on information about an individual that is publicly avail-

able and easily found (including a pet's name, a birthday, a child's name, or a mother's maiden name) or on widely familiar words and symbols (Nelson and Vu 2010).

An important reason for weak, low-entropy passwords is that consumers do not internalize all the costs of cybercrime. An individual consumer who chooses an easily defeated password puts not just her own privacy at risk but also the interests of others. Other consumers' identities are put at risk because there are fixed costs to hacking, and one consumer's negligence improves the joint return on a criminal's investment. One consumer's failure to take precaution (for example, failing to fix a broken window) can influence the chance that another consumer will be victimized (password precaution taking bears similarities to some auto-theft precautions; see Ayres and Levitt 1998). Retailers often bear the costs of reversing fraudulent transactions and resetting accounts, as well as reputational costs when their customers' accounts are hacked. The fraud insurance offered by retailers exacerbates consumers' moral hazard with regard to precaution taking—as witnessed in the greater reluctance of some consumers to share their Social Security numbers than their more-insured credit card numbers.[1] Thus, while consumers often experience the password requirements as a hassle, the retailer is well placed to trade off this dissatisfaction against the benefits of increased deterrence.[2]

An analogous story can be told with regard to sellers' precaution taking. Sellers, like consumers, do not by themselves internalize all the consequences of cybercrime attacks against their users but through the process of contracting are often willing to take on duties of precaution taking. The implementation of certification and secure payment systems (such as secure sockets layer certificates, Payment Card Industry Data Security Standards, or the HTTPS lock icon) can impose costs on retailers[3] but provide a potential benefit to consumers (and thus to the consumer-retailer pair).

1. This occurs even though Social Security numbers can be more at risk of third-party prediction than credit card numbers (Moore 2011–12). Starting with an individual's place and date of birth—at times knowable from a Facebook profile—a Social Security number can be probabilistically predicted by analyzing publicly available data containing the Social Security numbers of dead people.

2. The password mandates are just one way that sellers encourage consumers' password protection. The end-user license agreements at times incentivize consumer precaution by shifting liability "for loss of passwords due to user negligence" (Heartland Payment Systems 2016).

3. See, for example, Payment Card Information Security Standards Council, Securing the Future of Payments Together (https://pcisecuritystandards.org/).

The consumer and retailer jointly, through their contract, are therefore better placed to internalize more of the consequences of cybercrime. But to say that the consumer and seller are jointly better placed to trade off the costs and benefits of precaution taking is not to say that we should expect their contracts to impose optimal precaution levels. There are at least two reasons why we might expect that consumer-seller contracts would fail to incentivize sufficient precaution taking: uninternalized consequences and unobservable counterparty behaviors.

First, consider residual externalities. While there are often gains to trade in agreements imposing higher levels of precaution taking by both consumers and sellers, there are still consequences to cybercrime that are not internalized even by specific consumer-seller pairs. When Ashley Madison is hacked, consumers of other adultery websites (for example, Seekingarrangement.com) may become more reluctant to contract. News of cybercrime may therefore dampen commerce and impose costs beyond just the targeted retailer. Indeed, the consequences may be felt even in wildly different markets. The theft of consumer data from Target, for example, may make consumers generally more cautious about electronic transactions, impacting people beyond just those who had accounts at the compromised site and influencing their behaviors at websites even in different markets.

These inter- and intraindustry externalities also suggest that the employer-employee contracts may not mandate sufficient employee (or employer) precaution. In retail, mass loss of information from consumers' accounts is often caused by employee negligence. For example, after T. J. Maxx compromised the credit card information of 94 million customers, class-action litigation alleged that the retailer was responsible for employee negligence that led to the hacking (Schneider 2009). If the seller does not bear all the benefits of deterring the theft of information but bears all the costs of deterring the theft, we should expect undersupply of industry precaution against such hacks. The wholesale loss of consumers' identity information is an even larger policy concern than the retail concern of negligence of individual users to keep their passwords nonpublic.

The second reason for suboptimal precaution taking is the presence of counterparty behaviors that are difficult for the counterparty to observe, much less verify to an enforcing court. There are important observability limits to the kinds of precautionary obligations that a contract can impose on both consumers and retailers. The "contract" can require consumers to select strong passwords as a prerequisite to placing an or-

der, but sellers have a much harder time observing whether consumers have taken adequate care in keeping such information secure. Consumers who keep their passwords on easily found Post-its (hereafter, Post-it negligence) or who email their passwords to themselves or friends weaken the security of even very strong passwords.[4]

There is an inescapable tension between the kinds of consumer precaution that retailers can enforce and those that they cannot. Requiring nonintuitive passwords—for example, with numbers and punctuation marks—naturally makes it harder for consumers to remember their passwords and hence can lead the consumers to keep a written record of a password in a place that is sufficiently accessible for ready use. Requiring more precaution with regard to password entropy is thus very likely to induce less precaution with regard to consumers keeping a harder-to-remember password private. Given this tradeoff between password strength and Post-it negligence, it is somewhat surprising that more retailers do not leverage the beneficial inertia of default settings by offering passwords with higher entropy and easier-to-remember mnemonics—that is, by issuing an initial well-designed password that can be changed only with additional user effort.[5]

Another important unobservable behavior that can produce suboptimal precaution taking is the use by consumers of the same password on multiple websites. Because of consumers' tendency to reuse passwords, a breach of security at one site might give thieves the log-in information for a variety of other platforms. For example, Das et al. (2014, p. 1) find that "43–51% of users reuse the same password across multiple sites" and that a cross-site password-guessing algorithm "is able to guess 30% of transformed passwords within 100 attempts." A website's security might thus be significantly compromised by a breach of security at other websites. Password reuse is not only difficult for an individual site to observe; it also produces another externality reason as to why all the consequences of a security breach are not borne by the site that fails to protect its users' log-in information.

An individual website could take action against consumers' reuse of passwords by imposing idiosyncratic password requirements (for example, use of an internal numeral) that forces users to at least slightly modify

4. Improvements in biometric verification of identity (for example, by fingerprint or iris imaging) may radically reduce the prevalence of Post-it negligence.

5. My Crossfit Wodify account did this by initially choosing "doghappy34" as my default password, for example.

their standard password choices when registering for the site. Such idiosyncratic requirements might reduce password reuse negligence but again exacerbate the Post-it negligence mentioned above.[6] Alternatively, a website might require a user to promise not to reuse a password when registering and to give permission to verify compliance by allowing the retailer to log in on behalf of the consumer at other Internet venues. Someone from stickK should not be able to log in at other sites using your stickK email and password combination. Or at the time of registering, the stickK system might test a dozen other sites and reject any password that gains admission at other Internet platforms. One might even imagine retailer sites bringing suit against other sites that negligently allow the release of passwords that are likely known to be prone to reuse. For example, if Amazon could prove an increase in fraudulent transactions on accounts with users who also had been victims of a negligent release of data by another website, Amazon might reasonably claim to bear costs of the other site's negligence.

Finally, analogous problems of observability apply to sellers' precaution taking. Sellers' precaution taking, including precaution taking by retailers' employees, with regard to consumers' account information, log-in passwords, and credit cards, is largely a credence good. Individual consumers are ill-equipped to monitor and enforce contractual conditions. While third-party verification schemes may mitigate this problem, it also merely displaces the credence problem to another level.

In short, there are important aspects of consumers' behavior with regard to password reuse and password posting that are difficult for sellers to observe (much less verify to courts) and that thus preclude effective contracting. These noncontractible dimensions combined with the substantial consequences external to consumer-users predictably lead to suboptimal precaution taking by consumers.

3. A LAFFER CURVE OF (CYBER)CRIME

The foregoing analysis of private precautions takes as given particular levels of public precaution taking and government enforcement efforts, including expected punishments. Government enforcement efforts, of course, can vary and affect private precaution taking in important ways.

6. The reuse of security questions creates an analogous precaution externality. If hackers of one site learn answers to standard security questions (what was your first pet's name, in what city were you born), they may gain access to other otherwise secure sites.

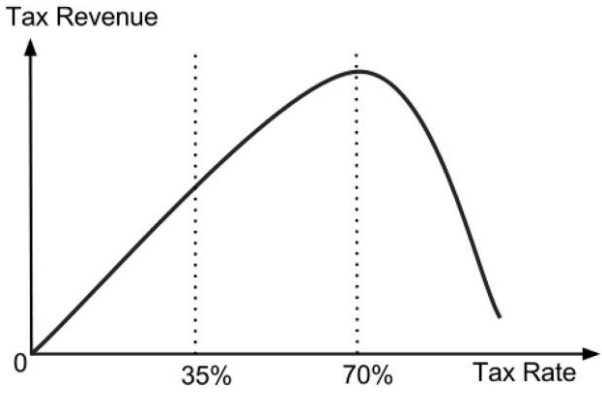

Figure 1. A Laffer curve

As Peltzman (1975) shows, for example, government-mandated precaution taking (for example, mandatory seatbelt wearing) can induce lower levels of private precaution taking (for example, safe driving).[7] In this section, I want to emphasize the interaction between the level of government precaution taking and the level of private precaution taking and private activity levels—both in contracting and in the amount of private information that consumers are willing to share with retailers (such as providing their credit card information, Social Security number, or friends' contact information).

My organizing analogy is to the Laffer curve: the Laffer curve—an example of which is in Figure 1—captures the notion that total revenues can decline, even as tax rates increase, beyond some sufficiently high level. The perverse (or downward-sloping) portion of the curve is due to the distortionary effect of the tax on the underlying activity. The underlying logic long predates Laffer's graphic representation. For example, as explained by Alexander Hamilton in *The Federalist,* no. 21, "If duties are too high, they lessen the consumption; the collection is eluded; and the product to the treasury is not so great as when they are confined within proper and moderate bounds" (Bartlett 2012, p. 1208).[8] In other

7. Peltzman (1975) describes the phenomenon wherein individuals adjust their behavior in response to the perceived level of risk, becoming more careful where they sense greater risk and less careful if they feel more protected, which results in a lower net benefit than expected.

8. Bartlett (2012) details that a host of writers, including the 14th-century philosopher Ibn Khaldun, Jonathan Swift, Adam Smith, and John C. Calhoun, understood that immoderately high tax rates could reduce total tax revenues.

Figure 2. A Laffer curve of crime

words, when taxes are too high, the curtailing reaction of private parties to the tax may so reduce commerce, in Hamilton's example import duties, that total tax revenue collected can decrease. The same might occur with income taxes. Just as the reduction of consumption activity can lead to the downward-sloping portion of the tariff Laffer curve, the reduction of work activity can lead to the downward-sloping part of the income-tax Laffer curve. The tax rate at which total tax revenue actually declines is disputed especially by politicians.

The Laffer curve has been applied to a few nontax contexts. For example, Claessens (1990) and others redeploy the idea in the context of country indebtedness to propose an analogous debt Laffer curve relationship between the nominal value of a country's debt and the total market value of the debt.

Here I want to suggest that there is also what might be thought of as a crime Laffer curve. As shown in Figure 2, the Laffer curve of crime relates the total amount of some particular crime to the expected punishment that an individual lawbreaker can expect to receive from breaking the law in question.

Like the original application to tax, the crime Laffer curve's perversity stems from the impact of the *X*-axis variable (the tax rate) on an underlying activity level. Where the perverse slope of the tax Laffer curve is the possibility of the downward-sloping portion of the curve when the value of the *X*-axis variable is high, the perverse slope of the crime Laffer curve is the upward-sloping portion of the curve when the value of the *X*-axis variable, the expected punishment in this case, is low.

The perverse possibility that, over some range, higher levels of ex-

pected punishment could increase the amount of crime stems from the possibility that, at very low levels of expected punishment, potential victims may reduce the activity levels that make them susceptible to victimization. For example, imagine there were very low expected penalties for mugging someone in the park at night. We might expect that few people would venture into the park at night. If government increased the expected punishment (by either increasing the probability of apprehension and conviction or by increasing the severity of the sanction conditional on conviction), potential victims might feel sufficiently safe to start returning to the park at night. Under such conditions, it is possible that increasing the expected punishment would lead to an increase in nighttime muggings.

From the perspective of the criminal, the perverse upward-sloping portion of the Laffer curve turns crime into a kind of Giffen good for which increasing the price (sanction) increases the quantity that criminals buy (commit). But whereas Giffen goods represent contexts in which the income effect dominates the substitution effect, the upward slope of the crime Laffer curve represents a context in which the victims' activity-level effect dominates the deterrence effect on criminals.

As the mugging example suggests, the possibility of a crime Laffer curve is not limited to cybercrime. But there are reasons to believe that the conditions of the perverse upward slope might be especially relevant with regard to the willingness of consumers to share their private information online with retailers. Some consumers have shown reluctance to engage in online commerce because they do not trust the retailers to keep their credit card information secure, even though they trust the servers at restaurants and other brick-and-mortar establishments. Other consumers are unwilling to save their credit card information with retailers or Internet providers for ease of subsequent purchases. Some users have furthermore (reasonably) sacrificed some features of smartphone applications (or the use of the applications altogether) because they are unwilling to log in through Facebook and possibly share their Facebook contact lists (Chatfield and Häkkilä 2004). In all of these circumstances, some parts of the online community may have seemed to some consumers like the nighttime park—a place where they refuse to go. The reduction in certain forms of online commercial activity might accordingly lead to the upward-slope perversity in which increasing the expected sanction (and therefore expected safety of the place) may lead to an increase in

total crime because of the disproportionate effect on consumers' activity (Smith and Vásquez 2015).[9]

So far, my use of the Laffer curve analogy has been descriptive. But there is an implicit normative corollary to the tax Laffer curve. If a policy maker finds herself on the perverse slope of the tax curve, she should reduce the tax rate. With apologies to the *Sound of Music,* the Laffer logic suggests that policy makers should "climb every perverse slope." In other words, if the tax rate is so high that it is depressing tax revenues, the tax rate should be lowered—doing so not only increases government revenue but also reduces the distortionary effect on taxpayers' behavior and allows them to retain more of their income.[10]

The Laffer analogy to crime would be less powerful if it were merely descriptive. But it turns out that a weaker form of this normative corollary (of climbing the perverse slope) for policy makers carries over to the criminal context: if a policy maker finds herself on the perverse-slope portion of Figure 2—that is, in that region wherein a move to increase the expected penalty for a crime also increases the incidence of that crime—the policy maker might at least presumptively consider increasing the expected penalty. Indulging even a rebuttable presumption of taking action to increase the amount of victimization from crime is normatively perverse. But to the extent that the upward-sloping portion of the crime Laffer curve is caused by changes in potential victims' activity levels, policy makers have reason to believe that the move to more crime benefits potential victims.

With regard to the mugging example, the perverse upward slope is caused by potential victims' willingness to return to the park, as perceived safety increases with expected sanctions. This increased activity level, in turn, induces higher amounts of crime. But the fact that potential victims return to the park reveals their preference to use the park more, even though doing so subjects them to a higher chance of victimization. Potential victims—after all—retain the ability to preclude the increase in crime (notwithstanding the increase in expected penalties) by simply con-

9. Smith and Vásquez (2015) formally model the equilibrium interaction among the expected penalty, citizens' precaution, and the level of crime and provide conditions under which an upward slope might pertain.

10. How far one should decrease the tax rate is less clear, however. Climbing to the top of the curve so as to maximize government revenue may not maximize efficiency. But following the Laffer logic that there are always (at least) two tax rates that will produce any given level of revenue, it should be clear that between (or among) equivalent tax-revenue-generating rates, the lower (lowest) rate is more (most) efficient.

tinuing to eschew the park. In other words, if they wanted to ensure their safety, they could just refuse to use the park.

Going to the park can be seen as both an increase in activity level and a reduction in basic precaution, but higher expected sanctions on perpetrators can also affect other forms of potential victims' precaution taking, such as keeping one's phone out of sight or walking briskly. A substitution between government and private precaution can have an analogous Laffer effect, as increased government enforcement may lead to reduced private precaution taking in ways that increase the equilibrium level of crime. The net effect on crime may turn, inter alia, on whether public and private precaution taking are strategic complements or substitutes (Bulow, Geanakopolis, and Klemperer 1985).

The preference of the populace inferred from activity and precaution choices for increased chance of victimization suggests that potential victims are presumptively better off by the increase in crime.[11] Of course, this revealed-preference argument depends on potential victims being sufficiently informed and rational about the expected risk of returning to the park (or to cyberspace). Government precautions—like the sellers' precautions mentioned earlier—are credence goods; it is difficult (if not impossible) for potential victims (like consumers) to monitor and measure their implementation and effectiveness to the degree necessary to make a completely informed decision. One important criticism of broken-windows initiatives is that they may mislead citizens into thinking that a renovated park is safer than it really is (Harcourt 2001). Even if the choice to return to the park (or e-commerce) itself is made under circumstances of incomplete or imperfect information, the choice nonetheless can provide evidence about what individuals expect will increase their utility.

Assuming hyperrational and perfectly informed citizens at best leads to nothing more than a policy presumption to climb toward more crime, because the foregoing revealed-preference argument leaves unaddressed the costs of increasing the expected sanctions. Even if citizens are made better off by moving to a portion of the curve with higher expected sanc-

11. An analogous story might be told with regard to other forms of public safety regulation that might increase citizens' activity levels. Thus, for example, a highway safety design mandate that so enhances the number of miles driven that it increases the number of car fatalities might be deemed, for analogous reasoning, to presumptively make drivers better off.

tions,[12] it is unclear whether those private benefits outweigh the social costs of higher expected sanctions. Moving to the right in Figure 2 normally will require hiring more police or prosecutors (to increase the probability of apprehension and conviction) or incurring more prison costs (to increase the penalty to those convicted). Any choice to increase the expected sanctions, therefore, should consider whether the presumptive benefit to potential victims is outweighed by the social costs of enhanced penalties.

Finally and most perversely, the undersupply of government precaution might ameliorate the undersupply of precaution produced by private contracting. While standard modeling of the interaction between government and citizens' precaution efforts assumes that citizens make optimal precaution decisions conditional on government action (Smith and Vásquez 2015), the first part of this argument suggests reasons why private contracting might produce suboptimal precaution given any particular level of government effort. Thus, the lessons of the two parts together might suggest that undersupply of government effort (such as through reduced expected punishments) might give rise to offsetting increases in private precaution taking. Therefore, even though third-party exploitation of password reuse (via Das et al. [2014] password-guessing algorithms) is the type of conduct that violates the core of the federal Computer Fraud and Abuse Act (18 U.S.C. 1030 [1986]), a less aggressive policy of enforcement might beneficially induce websites to guide users toward less reuse.

4. CONCLUSION

Section 2 argued that we might expect the level of precaution taking by consumers and sellers, with regard to online privacy, to be suboptimal (for any given level of expected government criminal enforcement) because of externalities and the existence of noncontractible behaviors. Section 3 used a Laffer curve to argue that when expected penalties are unusually low, potential victims might respond by reducing their activity levels by abandoning cyberspaces or failing to share otherwise valuable

12. While it is standard to discount the utility of the criminals, there is an analogous revealed-preference argument that consumers are made better off by moving up the perverse slope. Notwithstanding the increased activity level of citizens in the park, the criminals might have chosen not to mug—which indicates that they are better off mugging than not mugging (which is what they did when sanctions were lower).

information (such as credit card or contact details) because of concerns about safety. In such contexts, the welfare of the public (including both retailers and consumers) might be enhanced by a move toward higher penalties, despite the rise in crime that may result.

As in other contexts, however, the theoretical possibility of a Laffer curve perversity fails to provide concrete policy help. The normative payoff of a rebuttable presumption is of little use if policy makers are unable to divine whether the environment is operating at the upward-sloping portion. The most helpful clue would be for policy makers to look for massive activity-level effects whereby a substantial proportion of consumers decline for safety concerns to share what would otherwise seem to be valuable information. Even if policy makers were somewhat confident that the status quo policies placed the world on the perverse slope, it would be extremely unlikely that it would be possible to assess whether the private benefits from increased government effort would be worth the costs, especially given the results in Section 2 that showed that the private sector would undersupply precautionary contracting. In the end, the payoff of this piece is at most to suggest why efficiency analyses of cybercrime policies and marginal changes to such policies are likely to be infeasible.

REFERENCES

Ayres, Ian, and Steven D. Levitt. 1998. Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of LoJack. *Quarterly Journal of Economics* 113:43–47.

Bang, Youngsok, Dong-Joo Lee, Yoon-Soo Bae, and Jae-Hyeon Ahn. 2012. Improving Information Security Management: An Analysis of ID-Password Usage and a New Login Vulnerability Measure. *International Journal of Information Management* 32:409–18.

Bartlett, Bruce. 2012. The Laffer Curve, Part 2. *Tax Notes* 136:1207–9.

Bulow, Jeremy I., John D. Geanakopolis, and Paul D. Klemperer. 1985. Multimarket Oligopoly: Strategic Substitutes and Complements. *Journal of Political Economy* 93:488–511.

Chatfield, Craig, and Jonna Häkkilä. 2004. Designing Intelligent Environments—User Perceptions on Information Sharing. Pp. 570–74 in *Computer-Human Interaction,* edited by Masood Masoodian, Steve Jones, and Bill Rogers. Heidelberg: Springer Berlin Heidelberg.

Claessens, Stijn. 1990. The Debt Laffer Curve: Some Estimates. *World Development* 18:1671–77.

Das, Anupam, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014. The Tangled Web of Password Reuse. Paper presented at the Network and Distributed System Security Symposium, San Diego, CA, February 23–26.

Harcourt, Bernard E. 2001. *Illusion of Order: The False Promise of Broken Windows Policing*. Cambridge, MA: Harvard University Press.

Heartland Payment Systems. 2016. Online Privacy and Cookie Policy Statement. *Heartland*, June 27. https://www.heartlandpaymentsystems.com/privacy-policy/.

Ives, Blake, Kenneth R. Walsh, and Helmut Schneider. 2004. The Domino Effect of Password Reuse. *Communications of the ACM* 47(4):75–78.

Moore, Tara. 2011–12. Privacy Expert Uses Online Photos to Predict Social Security Numbers. *Engineering Magazine,* pp. 14–15. https://engineering.cmu.edu/alumni/magazine/winter_2011_2012/acquisti_privacy_predict_ssn.html.

Nelson, Deborah, and Kim-Phuong L. Vu. 2010. Effectiveness of Image-Based Mnemonic Techniques for Enhancing the Memorability and Security of User-Generated Passwords. *Computers in Human Behavior* 26:705–15.

Peltzman, Sam. 1975. The Effects of Automobile Safety Regulation. *Journal of Political Economy* 83:677–725.

Schneider, Jacob W. 2009. Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data. *Boston University Journal of Science and Technology Law* 15:279–303.

Smith, Lones, and Jorge Vásquez. 2015. Crime and Vigilance. Working paper. University of Wisconsin, Department of Economics, Madison.