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

*William K. Townsend Professor, Yale Law School. ian.ayres@yale.edu. Anthony Cozart provided helpful comments.
While many papers in this symposium are likely to focus on the efficiency of contracts authorizing retailers to use consumer data, another important use of contracts involves precaution 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 gains access not just to users personal information such as passwords and profile information but gains the ability to direct purchases to the hacker’s own benefit, the users loses autonomy and self-authorship. Identity theft is not just a species of privacy invasion, but it is a violation that is often much worse than the misappropriation concerns when retailers repurpose consumer information without sufficient consent. And unlike retailer misappropriation, third-party misappropriation often results in financial as well as autonomy related costs.

This article explores contracting between consumers and retailers affects precaution taking, and how this interacts with government policies to influence the prevalence of cybercrime. Specifically, it is posited that higher penalties may (counter-intuitively) produce more crime, but 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 in two parts: Part I discusses the precaution-taking incentives and provisions in consumer/seller contracts, and the possibility that externality and observability constraints will produce suboptimal precaution levels. Part II explores how this equilibrium between consumers’ and retailers’ behavior is likely to be influenced by different level of government precaution taking, and whether different policies could nudge precaution taking behavior in desired directions.

I. 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 each take precautions to prevent it. For example, when a website requires that a user register with a password that is at least 8 characters and contains at least one upper case, one lower case, and one number, the seller is requiring as a pre-requisite to contracting that the consumer engage in pre-caution taking that exceeds the level the consumer would otherwise choose to take. These precaution mandates alter consumer behavior. There is strong empirical evidence that a substantial number of users, left to their own devices, would choose extremely weak passwords.¹

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

¹ Users often use identical passwords across multiple accounts (Ives et al., 2004) (Bang et al., 2012) or passwords are frequently based on information about an individual that is publicly available and easily found (including a pet’s name, a birthday, a child’s name, or a mother’s maiden name in a password; CPP, 2009), or on widely familiar words and symbols (Nelson & Kim-Phoung, 2010).
defeatable, seemingly moronic, password puts not just her own privacy at risk, but also the interests of others. Retailers, for example, often bear costs of reversing fraudulent transactions and resetting accounts, as well as reputational costs when their customers’ accounts are hacked. Thus, while consumers often experience the password requirements as a hassle, the retailer is well-placed to tradeoff this dissatisfaction against the benefits of increased deterrence.\(^2\)

An analogous story can be told with regard to seller precaution taking. Just like with consumers, sellers by themselves do not 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 SSL certificates, Payment Card Industry Data Security Standard, 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).

The consumer and retailer jointly, through their contract, are therefore, better placed to internalizes more of the consequences of cybercrime. But to say that the consumer/seller are jointly better placed to take tradeoff 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 of 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 (e.g. 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 behavior at sites even in different markets.

These inter- and intra-industry externalities also suggest that the employer-employee contracts may not mandate sufficient employee (or employer) precaution. The retailer mass loss of information from consumer accounts is often caused by employee negligence. For example, after TJ Max lost the credit card information of 94 million customers, class action litigation

\(^2\) The password mandates are just one way that sellers encourage consumer password protection. The EULAs (End User License Agreements) at times incentive consumer precaution by shifting liability “for loss of passwords due to user negligence” (http://www.heartlandpaymentsystems.com/privacy-policy/).

alleged that that the retailer was responsible for employee negligence that led to the hacking. 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 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 contract can impose on both consumers and retailers. The “contract” can require consumer to select strong passwords as a prerequisite to placing an order, but sellers have a much harder time observing whether consumers have taken adequate care in keep such information secure. Consumers who keep their passwords on easily found post-its, or who email their passwords to themselves or friends, weaken the security of even very strong passwords.

There is an unescapable tension between the kinds of consumer precaution that retailers can enforce and those that they cannot. Requiring non-intuitive passwords – for example with numbers and punctuation marks – naturally makes it harder for consumers to remember their password, and hence can lead the consumers to keep a written record of the 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.

Another important unobservable behavior that can produce suboptimal precaution taking is the use by consumers of the same password at multiple websites. Because of consumers’ tendency to reuse passwords, a breach of security at one site might give thieves the login information for a variety of other platforms. (For example, it is possible that 10% of email/password combinations at my beloved stickK.com are identical to those users’ chosen passwords at Amazon.com or Facebook.com.) A website’s security might thus be significantly compromised by a breach of security at other websites. This is yet another reason why all the consequences of a security breach are not born by the site that fails to protect its users login information. An individual website could take action against consumers’ reuse of passwords by imposing idiosyncratic password requirements (e.g. use of an internal numeral) that forces users to at least slightly modify their standard password choice when registering for the site. Such idiosyncratic requirements might reduce password reuse negligence, but again exacerbate the “post it” negligence mentioned above. Alternatively, a website might require its users to promise not to reuse a password when registering and gaining the consumers’ permission to verify compliance by allowing the retailer to login on behalf of the consumer at other Internet venues. Stickk.com shouldn’t be able to log on at other sites using your stickK email/password

---

combination. Or at the time of registering, stickK might test a dozen other sites and reject any password that gains admission at other Internet platforms.

Finally, analogous problems of observability apply to seller precaution taking. Seller precaution-taking – including precaution-taking by retailer employees – with regard to consumer account information, login 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 consumer behavior with regard to password reuse and password posting which are difficult for sellers to observe (much less verify to courts), and which thus preclude effective contracting. These non-contractible dimensions combined with the substantial consequences external to consumer users predictably lead to suboptimal consumer precaution-taking.

II. 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. As Peltzman showed, for example, government mandated precaution-taking (e.g. mandatory seatbelt wearing) can induce lower private precaution taking (e.g. safe driving). In this section, I want to emphasize the interaction between the level of government precaution taking and private activity levels in both contracting, and in the amount of private information that consumers are willing to share with retailers (providing their credit card, social security number, or friends’ contact information, for example).

My organizing analogy is to the Laffer curve: The Laffer curve - an example of which is depicted in Figure 1 - captures the notion that total revenues can decline, even as tax rates increase, beyond some sufficiently high level. The “perverse” (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:

---

5 Peltzman described 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, resulting in a lower net benefit than expected. See, e.g. Peltzman, S. (1975). The effects of automobile safety regulation. The Journal of Political Economy, 677-725.
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.\(^6\)

In other 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 slope of tariff Laffer curve, the reduction of work activity can lead to the downward slope of income-tax Laffer curve. The tax rate at which total tax revenue actually declines is disputed especially by politicians.

Figure 1:

![Graph](Image)

The Laffer curve has been applied to a few non-tax contexts. For example, Stijn Claessens and others have redeployed the idea in the context 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.\(^7\)

Here I want to suggest there is also what might be thought of as a crime Laffer curve. As sketched in Figure 2, the Laffer curve of crime relates the total amount of some particular crime

---

\(^6\) Bruce Bartlett has detailed that a host of writers, including the 14\(^{th}\) century philosopher Ibn Khaldun, Jonathan Swift, Adam Smith and John C. Calhoun, understood that immoderately high tax rates could reduce total tax revenues. Bruce Bartlett, *The Laffer Curve, Part 2*, 136 TAX NOTES 43 (2012).

to the expected punishment that an individual law-breaker can expect to receive from breaking the law in question.

Figure 2: A Laffer Curve of Crime

![Laffer Curve of Crime](image)

Like the original application to tax, the criminal 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 taxation Laffer curve is the possibility of the downward sloping portion of the curve when the x-axis variable is high), the perverse slope of the criminal Laffer curve the upward sloping portion of the curve when the x-axis variable -the expected punishment, in this case - is low).

The perverse possibility over some range that higher expected punishments could increase the amount of crime stems from the possibility that - at very low levels of expected punishment - potential victims may reduce their 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 increase 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 where increasing the price (sanction) increases the quantity that criminals buy (commit). But whereas Giffen goods represent contexts where the income effect dominates the substitution effect, the upward slope of the criminal Laffer curve
represents a context in which the victims’ activity level effect dominates the criminals’ deterrence effect.

As the mugging example suggests, the possibility of a criminal 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 (or at least in the recent past were 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 login through facebook and possibly share their facebook contact lists. In all of these circumstances, 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 according 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 consumer activity.

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 policymaker 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.

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 (to climb the perverse slope) for policy makers carries over to the criminal context: If a policymaker finds herself on the perverse slope portion of Figure 2 – i.e. in that region wherein a move to increase the expected penalty for a crime also increases the incidence of that crime - the policymaker might at least presumptively consider increasing the expected penalty. Indulging even a rebuttable presumption of taking

---

9 Lones Smith and Jorge Vasquez have formally modelled the equilibrium interaction between the expected penalty, citizen precaution and the level of crime and provided conditions under which an upward slope might pertain. See Lones Smith & Jorge Vasquez, Crime and Vigilance, working paper (July 21, 2015).
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.
action to increase the amount of crime victimization is normatively perverse. But to the extent that the upward sloping portion of the criminal Laffer curve is caused by changes in potential victims’ activity levels, policymakers have reason to believe that the move to more crime benefits potential victims.

Returning to the park 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 a 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 continuing to eschew the park. In other words, if they wanted to ensure their safety, they could refuse the use the park at all.

The preference of the populace inferred from their activity choices for increased chance of victimization suggests that potential victims are presumptively better off by the increase in crime. Of course, this revealed preference argument depends on potential victims be sufficiently informed and rational about the expected risk of returning to the park (or to cyberspace). Government precautions – like the seller 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. 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 of about what individuals expect will increase their utility.

Even if the citizenry were hyper-rational and perfectly informed about the risk of crime, the normative case for climbing toward more crime can be at best no more than a presumption, 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 sanctions, 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

---

11 An analogous story might be told with regard to other forms of public safety regulation that might increase citizen 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.


13 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 – indicating that they are better off mugging than not mugging (which is what they did when sanctions were lower).
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 citizen precaution efforts assume that citizens make optimal precaution decision conditional on government action, Part I suggested reasons why private contracting might produce suboptimal precaution taken 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 -- although the motivating example of the empty park suggest that undersupply of government effort will exacerbate inefficient activity levels.

Conclusion

Part I 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) due to externalities and the existence of non-contractible behaviors. Part II used a Laffer curve to argue that, when expected penalties are unusually low, potential victims might respond by reducing their activity level by abandoning cyberspaces or failing to share otherwise valuable information (such as credit card or contact details) because of concerns about the safety of the space. In such contexts, the welfare of the public (including both retailers and consumers) might be enhanced by a move towards higher penalties, despite the rise in actual 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 policymakers are unable to divine whether the environment is operating at an upward sloping portion. The most helpful clue would be for policymakers to look for massive activity level effects whereby substantial proportion of consumers decline for safety concerns to share what would otherwise seem to be valuable information. Even if policymakers 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 costs -- especially given the undersupply contracting result of Part I. 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.

14 See, e.g., Smith & Vasquez, supra note 9.