Spare the Rod, Spoil the Network Security? Economic Analysis of Sanctions Online

Vaibhav Garg
School of Informatics and Computing
Indiana University
Bloomington, IN USA 47405
Email: gargv@indiana.edu

L. Jean Camp
School of Informatics and Computing
Indiana University
Bloomington, IN USA 47405
Email: ljcamp@indiana.edu

***Abstract*—When and how should we encourage network providers to mitigate the harm of security and privacy risks? Poorly designed interventions that do not align with economic incentives can lead stakeholders to be less, rather than more, careful. We apply an economic framework that compares two fundamental regulatory approaches: risk based or *ex ante* and harm based or *ex post*. We posit that for well known security risks, such as botnets, *ex ante* sanctions are economically efficient. Systematic best practices, e.g. patching, can reduce the risk of becoming a bot and thus can be implemented *ex ante*. Conversely risks, which are contextual, poorly understood, and new, and where distribution of harm is difficult to estimate, should incur *ex post* sanctions, e.g. information disclosure. Privacy preferences and potential harm vary widely across domains; thus, post-hoc consideration of harm is more appropriate for privacy risks. We examine two current policy and enforcement efforts, i.e. Do Not Track and botnet takedowns, under the *ex ante* vs. *ex post* framework. We argue that these efforts may worsen security and privacy outcomes, as they distort market forces, reduce competition, or create artificial monopolies. Finally, we address the overlap between security and privacy risks.**

I. Introduction

Böhme et al. [1] have presented economically rational arguments for the market to self regulate[1] and provide adequate privacy preserving mechanisms. In practice, however, this self regulation is only marginally true for specific markets [3], and even then providers often choose not to advertise better data collection practices [4]. Thus, there is a market of lemons in privacy, and vendors who make misleading privacy claims are often commercially successful [5]. The phenomena of a lemon's market also impinges security solutions [6]. Even with clear market signals, individuals may be rationally incentivized to free ride than invest in security solutions [7].

To prevent this tragedy of the 'information' commons [8], security of a network can be viewed as a public good [9], a private good with externalities [6], or a common-pool resource [10], wherein security and privacy guarantees are provided by peers [11]. All three regimes, irrespective of their grounding in public goods, private goods, or common-pool resources, leverage the notion of sanctions. The agency responsible for implementing these sanctions, however, differs based on the nature of the (security) good. A sustainable solution would aim to reduce the costs of regulation and enforcement for the responsible agency, be that government actors, independent coordinated stakeholders, or market forces of supply and demand.

There are two kinds of regulatory regimes for sanctions regardless of the regulatory approach [12]: 1) *ex ante* and 2) *ex post*[2].

Ex Ante, or action-based sanctions, is a system that prohibits specific actions. For example, in automobile safety, *ex ante* regulation manifests as speed limits, where it is considered too dangerous for individuals to drive above a certain limit. It does not matter if no one is being harmed in an instance of speeding. It remains prohibited. Online these sanctions manifest as policy initiatives like Do Not Track (DNT) [15]. DNT prohibits tracking individuals who express a preference against it, irrespective of whether data collection would lead to a potential privacy violation. Thus, *ex ante* sanctions are action dependent regardless of harm.

Ex post, or harm-based regulation, are sanctions after the fact. For example, if a driver causes an accident the corresponding sanctions are based on the resulting harm, independent of whether the driver was speeding, drunk, etc. An example of such sanctions may manifest in higher insurance rates. Thus, *ex post* sanctions are harm dependent. If a potentially hazardous activity does not have any negative consequences, there are no sanctions. Online these sanctions manifest as FTC enforcement against Google for privacy breaches due to Buzz [16]. Similarly, McColo shutdown by Global Crossing and Hurricane Electric was an ex post market sanction[3].

Currently both *ex ante and ex post* regimes are being used to develop policy responses to security and privacy risks online. These sanctions have been enforced by agencies such as Federal Bureau of Investigation and Federal Trade

[1] An example of self-regulation is the Payment Card Industry Dare Security Standard (PCIDSS), which is a set of guidelines to protect credit/debit card data put forth by VISA, Mastercard, and other credit card companies [2].

[2] A third option is mandated information disclosure to reduce information asymmetries in the market thereby allowing competition between firms that implement strong security/privacy controls vs. those that do not. In this paper we assume that information disclosure is similar to ex post sanctions in that it leads to reputation loss after a breach has occurred. Previous research has investigated the relative economic merits of ex ante, ex post, and information disclosure regimes for privacy breaches [13]. This research differs in three aspects. First, previous work models the cost of privacy breaches and not the benefits from information collection. Second, prior research focused on privacy and not security breaches. Finally, they assume that harm from a breach is uniformly distributed amongst the population. However, privacy concerns and therefore harm differ based on the population [14].

[3] http://arstechnica.com/security/2008/11/spam-sees-big-nosedive-as-rogue-isp-mccolo-knocked-offline/, Retrieved Jan 30th 2015.

Commission (FTC), where the latter is simultaneously being tasked with creating and enforcing policy. The actions of both these agencies, in enforcement as well as policy, have been controversial. FTC supported ex ante co-regulatory approaches, such as Do Not Track, have been under attack from both who are privacy advocates [17] and those who prefer the free market approach [18]. Similar privacy regulations in the European Union have alleviated the impact of online advertising [19]. Simultaneously, badly designed sanctions can limit consumer choices in privacy enhancing technologies. For example, filters that reduce the amount of advertising spam, increasing the effectiveness of behavioral targeting, may demonstrate behaviors similar to spyware and thus may be considered illegal [20].

In security private organizations engage in various forms of ex ante sanctions and ex post costs. Peering agreements which though not public, provide an avenue for ex ante sanctions not unlike automobile insurance. Alternatively in payment processing, there are ex post sanctions in the forms of higher future rates for past fraud. However, ex post sanctions in security, e.g. takedowns of botnets (e.g. Nitol) co-ordinated by the FBI and private stakeholders such as Microsoft, can lead to collateral damage [21]; while ex ante regulations proposed by the FBI, such as CALEA II, may further degrade both the security and privacy properties of the Internet [22].

Given that both ex ante and ex post sanctions can be used, which are more effective and economically sensible for security and privacy risks online? In this paper we begin to answer this question by using an economic framework that compares the effectiveness of these two distinct regimes for environmental risks [23]. Security and privacy risks are similar to environmental risks in that they have components of *public goods, private goods with negative externalities, and common pool resources* [10]. **Our analyses indicate that current policy solutions may worsen security and privacy outcomes, by reducing competition and (often) creating artificial monopolies. Thus, we suggest appropriate regulatory regimes contingent on four factors: 1) whether services are perfect substitutes, 2) availability of robust market signals, 3) presence of network effects, and 4) cost of enforcement.**

We begin by introducing the general economic model of sanctions [23] in section II. Section III extends this model by considering an inequitable distribution of risk. In section IV we analyze case studies of current policy solutions using the economic framework, specifically Do Not Track and botnet takedowns. Section V discusses the broader scope of sanctions and the implications for public policy. We also provide specific insights for enforcement agencies. Finally, section VI concludes with a summary of our findings and discussion of future work.

II. General Model

This section introduces, translates, and applies an economic model of ex ante and ex post sanctions posited by Garoupa et al. [23] to security and privacy risks online. They assume that the harm due to an activity is not certain and is difficult to predict ex ante. They also assume that assessing the harm ex post is costless. The harm of security and privacy risks is neither certain nor easily quantifiable before a breach or violation. For example, all software are deployed despite a variety of vulnerabilities. However, it is hard to predict ahead of time which ones would be exploited by the attacker. Similarly, personal information is collected by many websites for advertising. However, it is difficult to predict which provider is likely to suffer a privacy breach. (Some of these difficulties are documented in the cyber-insurance literature [24].) However, after a breach it is relatively easier to quantify the damage, e.g. in terms of number of personal records stolen. (Note that this is not a comprehensive conceptualization of harm. For example, this does not take into account chilling effects [25].)

The benefit from the harmful activity is given by b. Arguably, if there is no benefit there is no economic rationale to engage in an activity. For example, while data collection can lead to privacy and security breaches, it also provides companies competitive advantage through price discrimination, product differentiation, and behavioral targeted advertising [26], albeit small [27]. The resulting transactions from such activity also increases the welfare of individuals. For example, price discrimination and product differentiation allows individuals to get the products they want at a price they can afford. Thus, we are concerned both with the relative cost-benefit analysis of individual companies under different sanctioning regimes as well as the net impact on social welfare. Social welfare is as defined by Polinsky et al. [28], i.e. g(b) is the density of benefits between individual companies and **G**(b) is the cumulative distribution from [0,B].

The probability of the security/privacy risk of an activity manifesting is given by σ, where $0< \sigma <1$. The corresponding harm is quantified by h. The expected value of a harm is σh. σ is estimated by individuals as σ_e and by government as σ_g. σ refers to the true value of the estimate. For the general framework we cover perfect information ($\sigma_e = \sigma_g = \sigma$) as well as imperfect but symmetric information ($\sigma_e = \sigma_g \neq \sigma$). The probability of prosecution and enforcement is given by p, where $0< p <1$.

First consider the *ex ante* regime. Let f be the fine imposed by the government for an activity that can lead to a security or privacy violation. Offline, for example, such fines can manifest as speed limits on roads. Online, a analogy may be mandating a minimum level of encryption routers. The state of Nevada, for example, mandates that if a business transmits personal information to a contractor it has to be encrypted [13]. These mandates may also be implemented via industry standards, e.g. Payment Card Industry Data Security Standard [2]. (Sometimes such fines can be vague. For example, under the Information Technology Act in India, companies can be held liable in a civil court if they failed to provide a minimum level of security for their databases [29]. However, this 'minimum level of security' is not specified and is evaluated *ex post*.)

The canonical example for *ex ante* privacy sanction in United States would be Health Insurance Portability and Accountability Act (HIPAA) [30]. Given that the sanction through HIPAA is given by f and the probability of detection and prosecution is p, the expected sanction would be pf. We assume that companies are risk neutral. Then it is only economically rational for a company to engage in an activity if $b - pf > 0$ or $b > pf$. The impact of that activity on social welfare, given *ex ante* sanctions, is quantified by equation 1. On solving the first order condition [23], sanction $f = \sigma_g h/p$.

$$W_U = \int_{pf}^{B} (b - \sigma_g h) dG(b) \quad (1)$$

Now consider the *ex post* regime. Let s be the fine imposed by the government for an activity that can lead to a security or privacy violation. Offline such sanctions were imposed, for example, on British Petroleum after the oil spill [31]. An online analogy would be the sanctions imposed on Google after its deployment of the Buzz Social Network [16]. Similarly, the FBI used its enforcement powers to seize the servers of 3322, which was one of the dynamic DNS provider used by the Nitol botnet [21].

Given that the enforced sanction by the FBI or FTC is s, the probability of harm is σ, and the probability of detection and prosecution is p, the sanction imposed would be σps. Since we assume that companies are risk neutral, then for an activity to be economically rational $b - \sigma_e ps > 0$ or $b > \sigma_e ps$. The corresponding impact on social welfare, given *ex post* sanctions, is given by equation 2. Solving the first order condition [23], sanction $s = \sigma_g/\sigma_e \times h/p$. *Clearly, deterrence is higher under harm-based sanctions vs. actions based sanctions if $\sigma s > f$, and vice versa.*

$$W_U = \int_{\sigma_e ps}^{B} (b - \sigma_g h) dG(b) \quad (2)$$

Ex ante sanction is $f = \sigma_g h/p$, while *ex post* sanction is $\sigma_g/\sigma_e \times h/p$. *Thus, we can say that the sanction, and corresponding deterrence, is higher ex post than ex-ante.* Becker [32] notes that if the fine post conviction is \$x, then the individual (facing potential conviction) would be willing to spend \$x to avoid prosecution. In Becker's analysis this manifests as bribery. However, bribery is merely a mechanism that alleviates the probability of detection and prosecution. Online the alternative, which provides the same overall reduction in prosecution, can be post hoc investment in technologies that mitigate harm.

TABLE I. TABLE OF SYMBOLS

b	the benefit of risking the creation of harm to the decision-making party
h	harm corresponding to the risk occurrence
p	probability of detection and prosecution for that harm
σ	probability of harm occurring given risk
$v(\sigma_e)$	density distribution of the probability of harm
σh	expected value of the harm
σ_e	individuals' estimate of their own harm
σ_g	government estimate of individuals' harm
W_U	impact of harm on social welfare
f	fine to decision-maker under ex-ante given violation of requirements
s	fine to decision-maker under ex-post given existence of harm

It is well established in economic literature that sanctions under a harm-based regime are higher than under action-based regime, i.e. there will be higher investment in risk mitigation technologies under a harm-based regime. (Contested well established economic findings is beyond the scope of this work, rather we are applying these theories in the domain of privacy and security.) For example, investments can be made in training personnel, providing appropriate security solutions at subsidized costs, providing incentives for individuals to comply with company security policy etc. Such investments would typically impinge the probability of the breach. *It has been shown that under certain conditions insolvent injurers do in fact (over) invest in harm mitigation technologies [33]. Thus, under harm-based sanctions consumer protection would be higher, even if social welfare is the same ex post as well as ex ante.* (Unfortunately while there is over investment in technologies that reduce the probability of harm, similar investments to alleviate the magnitude of harm are found wanting.)

However, this finding is limited by judgment-proofness. Judgment-proof firms are those that can suffer accidents but do not have adequate financial resources to recompense the victims [34]. Online, for example, medical records firm Impairment Resources LLC was forced to file for bankruptcy when private information of 14,000 patients was breached [35]. Potential injurers as such may then become less cautious [36].

There are, however, solution to firms being judgement-proof. First, lenders to such firms can be made more liable. However, it has been shown that increasing liability for the lender increases the probability of accidents/breaches and lowers social welfare [34]. A second solution then is to combine monetary fines with non-monetary sanctions. For example, in the Google Buzz settlement in additional to the financial fines Google was also required to put in place a comprehensive privacy program. However, there can be an upper bound on non-monetary sanctions under the law. For example, in certain countries such as Spain and Norway there is an upper bound on the length of the jail term [37].

In general, judgment-proofness is less of a concern for companies that collect and store data on a large scale. The harm caused by a breach that leads to data disclosure would have the monetary upper bound as quantified by the financial worth of the database. Thus, even if the company were to go bankrupt they can arguably sell their databases as assets to recompense the injured party. FTC, however, has prevented such transactions from happening in the past. For example, FTC limited Toysmart's ability to sell its consumer database to a qualified buyer, where the 'qualified buyer' had to be another company that sold toys [38].

Firms that do not collect consumer information as assets may however be judgement-proof. For example, dynamic DNS providers such as 3322.org do not collect consumer information, compared to a company such as Google (whose business is grounded in the advertising model). Thus, if *ex post* sanctions are so high that 3322.org is rendered bankrupt; then these sanctions would create an economic disincentive for dynamic DNS providers, and other similar network service providers such as ISPs, to engage in due diligence [36]. Sanctions for such entities must be carefully designed so as to mirror the conditions under which there is (over) investment in risk mitigating technologies, e.g. those assumed by Dari-Mattiacci et al. [33]. However, even then there is over investment in technologies that mitigate the probability of harm, while investment in those technologies that impinge the magnitude of harm is limited. For social welfare this is a sub-optimal condition. *Therefore, when firms are judgment-proof*

the appropriate solution is to encourage ex ante sanctions.[4]

For both *ex post* and *ex-ante* cases the expected sanction is determined by the perception of the government and given by $\sigma_g h$. Thus, social welfare is the same under both conditions. Ex-ante sanction, as determined by the absolute perceptions of the government, could be over-estimated, for example in the presence of path-dependence [39], or underestimated, e.g. if the harmful act is new. Arguably, security and privacy breaches are relatively novel; for example, compared to health risk. As such, databases of security and privacy breaches are limited. It was only in 2002 that California for the first time required companies to notify their customers of data breaches. The construction of a framework for cyber-insurance has been impacted by the difficulties of developing an actuarial model that can adequately estimate either the probability or magnitude of harm for security and privacy risks online [40]. *Thus, it is likely that under action-based sanctions fines will be under-estimated and therefore socially suboptimal in terms of deterrence*.

As such under an *ex ante* as well as *ex post* regime the sanction is determined by the perceptions of the government. However, when the individual estimate of the probability of harm is the same as of the government, i.e. $\sigma_e \approx \sigma_g$, the sanction *ex post* is simply h/p. Therefore, when the perceptions of the government are close to reality *ex post* sanctions are more stable. In general, *ex post* sanctions are determined by the court and can be adjusted on a case by case basis till the optimum results is reached. *Ex ante* sanctions are, however, are prescribed by the legislature and thus any change is (prohibitively) expensive. Thus, under an *ex ante* regime there is increased pressure (or costs) for the enforcement agency to ensure that sanction is not underestimated or overestimated.

Simultaneously, the number of prosecutions is higher under an *ex ante* regime than an *ex post* one. If the cost of prosecution is zero this difference is inconsequential. However, prosecution is rarely costless in the real world and online risks often bring additional costs of cross-jurisdictional prosecutions. Anderson et al. argue that for cybercrime the cost of deterrence may be much higher than the financial impact of undesirable activity [41]. The problems inherent in online fraud prosecutions are well documented [42]. *Thus, given the expense of prosecuting security and privacy violations online, ex post sanctions are potentially more economically efficient than ex ante sanctions*. (Note that in practice courts have done a poor job of recognizing privacy harms due to breaches, though tangible losses do result in damages being awarded [13].)

III. Non-uniform distribution of risk

The general framework makes the assumption that the harm caused by an accident is uniformly distributed across the population. However, this is not true either offline or online. For example, offline a chemical spill would impact those with limited economic resources as well as those who are closer to the source of the spill more. Similarly online the harm of a security or privacy breach is not equally distributed. Privacy arguably is more relevant for marginalized communities and traditionally vulnerable communities. For example, a weakness in privacy controls allowed for the creation of the mobile application Girls Around Me [43]. It is unlikely that a similar application targeting men would emerge. Loss of privacy may be more important for member of LGBTQ community[5], who may suffer both social discrimination as well as physical violence. Financial loss from a phishing attack may be more relevant for older adults. Adults over 65 would have less time and ability to replenish lost money compared to younger cohorts. Finally, concerns about privacy are not spread uniformly, i.e. individuals are more concerned about protecting undesirable traits [14].

Thus, the framework extension in this section assumes that the probability of harm, σ_e, varies across the population with a density distribution $v(\sigma_e)$ and cumulative distribution $V(\sigma_e)$. It is expensive to know individual probabilities. However, the distribution is known to the government. Under these constraints expected social welfare is redefined in equation 3 for *ex ante* and 4 for *ex post* sanctions [23]. The *ex ante* sanction f is then recomputed as $\sigma_g h/p$. Simultaneously, the *ex post* sanction s becomes $\rho\sigma_g h/p$, where ρ is $\int_0^1 \sigma_e g(p\sigma_e s)dV(\sigma_e)$ divided by ρ is $\int_0^1 \sigma_e^2 g(p\sigma_e s)dV(\sigma_e)$; $\rho > 1$.

$$W_V = \int_0^1 \int_{pf}^{B} (b - \sigma_g h)dG(b)dV(\sigma_e) \tag{3}$$

$$W_V = \int_0^1 \int_{\sigma_e ps}^{B} (b - \sigma_g h)dG(b)dV(\sigma_e) \tag{4}$$

The expected sanction then changes. For action-based sanctions the expected sanction, $\sigma_g h$, is still defined by the perceptions of the government. For harm-based sanctions the expected sanction will be $\sigma_e \rho \sigma_g h$. Then individuals for whom $\sigma_e < 1/\rho$, the expected sanction is higher under an action-based regime. However, for others the sanction is higher under a harm-based regime. The net social welfare if both action-based and harm-based sanctions are used is given by equation 5.

If $\sigma_g \approx \sigma$ equation 5 is positive. Thus, harm-based sanctions are strictly preferred. If, however, σ_g is overestimated or underestimated 5 could be negative. Then action-based sanctions would be strictly preferred. If σ_g is overestimated, since the expected sanction for action-based sanctions is a function of the perceptions of the government, the second term in equation 5, would be positive. Thus, the first term could be negative. If the absolute value of the first term is greater in magnitude than that of the second term, harm-based sanctions would be strictly preferred. Alternatively when σ_g is underestimated the first term is always positive. In this case

[4]Romanosky et al. [13] reached a similar conclusion. Note that their model differs from one presented here, in that they model on the costs of privacy breach and not its benefits. A security breach for an organization like 3322.org arguably does not demonstrate benefits for either 3322.org or its customers, i.e. bots on 3322.org do not create positive externalities for the network. Thus, we argue that when consumers do not benefit from activities that expose them to security/privacy risks ex ante sanction may be more socially optimal.

[5]LGBTQ refers to lesbian, gay, bisexual, transgendered, and queer community, i.e. individuals who do not adhere to traditional normative heterosexual behaviors.

the second term can be negative and greater in magnitude compared to the first term. Here again harm-based sanctions would be strictly preferred.

$$\delta W_V = \int_0^{1/\rho} \int_{\sigma_e \rho \sigma_g h}^{\sigma_g h} (\sigma h - b) dG(b) dV(\sigma_e) + \int_{1/\rho}^{1} \int_{\sigma_g h}^{\sigma_i \rho \sigma_g h} (b - \sigma h) dG(b) dV(\sigma_e) \tag{5}$$

In general when the government has accurate perceptions about the probability of harm, action-based or ex ante sanctions are appropriate. However, new activities for whom not enough information is available should be regulated with harm-based or ex post sanctions. For security and privacy we can identify the risks for whom harm is not uniformly distributed across the population. For such risks we can partition into two types. **First, there are activities for which there is significant data that the risks can be fairly well characterized. Second, there are activities, particularly those that are new but also those for which there are no data or are inherently unobservable, whose risks are not readily available.**

IV. An Analysis of Current Policy Efforts

In this section we analyze two current policy initiatives using the economic framework introduced in previous sections. Specifically, we examine one privacy policy initiative that imposes *ex ante* sanctions in terms of reputation loss for the provider. We also investigate a security policy initiative that posits *ex post* sanctions by disrupting the services of the network provider.

A. Case Study 1: Do Not Track (DNT)

Do Not Track (DNT) is a proposal that allows users the right to opt out of behavioral tracking online [15]. There have been several criticisms of this proposal. On the technical side it has been argued that there are other ways to track individuals that have not been covered by this proposal, e.g. browser fingerprinting [44]. On the economic side it has been argued that it is infeasible for the market to function (efficiently) without adequate information [45].

DNT is a reputation based sanction. It allows the user to set a flag whereby websites that honor DNT will no longer collect a specific set of information from the privacy sensitive user. If the website does not respect the expressed preference of the user, it would suffer a reputation cost. For example, the user may then switch to a website that does comply with DNT. (If Google refuses to company with DNT, the user has the option to switch to Microsoft's Bing or DuckDuckGo. For example, post PRISM revelations DuckDuckGo reportedly saw a 50% increase in web traffic to its search engine [46].)

For the purpose of this discussion we will assume that privacy is a social good that is needed [47] and the DNT in fact works, i.e. DNT is technologically adequate or at least is an improvement over status quo. Given these assumptions is DNT the best possible, i.e. economically efficient, policy solution? Could the same amount of privacy protection have been achieved through another policy with lower costs? Or alternatively could greater privacy protection have been possible, given the same costs, under a different policy? Thus, what is the opportunity cost of DNT? Specifically, would a harm based sanction be preferred for being economically efficient?

DNT is an *ex ante* sanction, i.e. websites are prohibited from collecting a specific kind of information. As noted for the general framework (i.e. section II), the harm of collecting information for behavioral targeting is not certain. However, it is possible that information collected might be accessed by unauthorized agencies. For example, it is possible for a company to collect information stating that they would not share the information with third parties, but then change the terms of use later. Alternatively, the agency collecting information may get hacked by cyber-criminals. Finally, undesirable behavioral advertising may reveal information that an individual may wish to conceal. (In the past such disclosures have included instances where parents found out that their daughter was pregnant [48].) A broader adversarial model might incorporate state actors, where information collected by private agents is made available to government actors, with or without adequate administrative oversight, e.g. PRISM [49].

As we note in section II, action-based sanction implies that companies may spend less resources on harm mitigation technologies. In the case of DNT the websites that comply will arguably have a reduced ability to deliver behavioral targeted advertisement. Lets assume a market with two players, A and B, whose products are perfect substitutes. Then the player who cannot deliver targeted advertisements would sell less of their product. Simultaneously, they will save on the cost of delivering targeted advertisements. Arguably, the saving on advertising would always be lower than the revenues from selling extra goods or services. (Otherwise it would not be economically rational to engage in advertising at all.) Thus, the player that complies would be at a loss. Consequently, they would have fewer resources to invest in harm mitigation technologies or to provide for *ex post* sanctions.

Let us consider the scenario from the perspective of the player B who does not comply. Lack of compliance will provide additional revenue from behavioral targeting. Simultaneously, there would be a reputation cost associated with the player B. If player B has a substantial number of customers who are concerned about privacy, they may choose to with to the product from player A. However, if switching costs are high individuals may simply stop using the product from player B without investing in player A. For example, moving from Facebook to Google Plus may have prohibitive costs due to network effects [50], i.e. the worth of Google Plus' social network is determined by the number of individuals on the network; if all my friends are on Facebook, there is (approximately) zero benefits of joining and high costs of switching to Google Plus. Alternatively, individuals who are concerned about Facebook's privacy violations may simply stop using that social network without moving to a new one; this too would have high costs albeit social ones. A trivial example is that of party invitations, which are sent on Online Social Networks (OSNs). If an individual is not on the revenant OSN, their friends would (unintentionally) forget to invite them. Higher economic costs would be seen when such interactions lead

to loss of, for example, employment opportunities. The cost of privacy violations to the service provider themselves are limited, and even negligible. For example, it has been shown that while a company's stock value goes down after a breach, the impact is limited in time; i.e. the loss is recovered within a matter of days [51].)

In general, the risks of information sharing are not evenly distributed over the population. Simultaneously, these risks are often new. Thus, government agencies will likely underestimate *ex ante* sanctions. Such sanctions also impinge on the firms' ability and incentives to make post hoc investments in harm mitigation technologies. Here we have not modeled other factors such as market competition. However, it is not difficult to see that *ex ante* sanctions would increase the cost of entry in the market, which would decrease the number of independent market players, thereby decreasing competition (on privacy). (In fact, given that DNT is a self governed body constituting mostly of major incumbent market players, with a nominal FTC presence, suggests that the industry wants a token regulation in place to prevent functional alternatives, while increasing the costs for new entrants.) Given the analysis in this section it is likely that harm-based sanctions would be preferred for privacy risks in most contexts. (Arguably the influential regulation, which has driven better privacy protections in the market has been harm based, i.e. the legislation which requires companies to inform users of information loss in the case of a data breach.)

B. Case Study 2: Botnet Takedowns

Recently, the FBI has been involved in highly publicized takedowns of several botnets. Typically, these takedowns are joint operations between the FBI and private entities such as Microsoft, Paypal etc. For example, FBI brought down 3322.org a dynamic DNS provider in a joint operation with Microsoft. 3322.org was targeted as it was hosting a large number of systems in the Nitol botnet.

These takedowns have been criticized on two accounts [21]. First, it has been argued that these takedowns have limited impact on the botnets. In fact these partial takedowns harden the botnet operators further against future takedowns. A second argument is about the collateral damage of takedowns. 3322.org was not the only dynamic DNS provider related to Nitol bots. Simultaneously, 3322.org was not exclusively used by Nitol bots. In fact there was a large legitimate user base whose services were disrupted when the servers for 3322.org were seized. (3322.org was being used by small to medium sized businesses who wanted a cheap hosting solutions. The disruption of services would have caused tangible financial loss, e.g. customers being unable to submit orders online.)

Here we gloss over previous criticisms. Much like in the previous case study, here we are concerned with the opportunity costs of take downs. Could the resources used for takedown have been allocated under a different policy to get better security for the network? Specifically, would an action-based or ex ante sanction be preferred (or be more economically efficient)?

Botnet takedowns of offending ISPs or dynamic DNS providers are akin to a harm-based sanction. Law enforcement, in collaboration with private actors, identifies which network operators have a bad track record, for example, of hosting phishing websites. These operators are sanctioned by disrupting the network services they provide. Here again the harm from being part of a specific provider is not certain. For example, just because an individual was hosting services using 3322.org does not imply that they are in fact a member of the Nitol botnet. However, it is more likely compared to when services are hosted on a more security aware dynamic DNS provider.

As noted before, harm-based sanctions are limited when firms are judgment-proof. This is a concern for organizations such as 3322.org. For example, 3322.org has to provide consumer support for the legitimate users whose services are disrupted when FBI conducts a takedown. Unless 3322.org has the financial resources to provide such customer support, the cost would have to be borne by an external agency. Alternatively, legitimate consumers would lose their services without being adequately compensated. Given two dynamic DNS service providers in perfect competition, if one is more concerned about the nature of the code being hosted that entity would find less number of customers. Arguably, a higher concentration of malware would make the dynamic DNS provider less valuable as they are more likely to be on blacklists. Note that unlike in the previous case study two dynamic DNS providers are perfect substitutes. Hosting on a specific provider is not technologically better than another one. (For OSNs this is not true due to network effects.)

However, disruption of services eliminates this naturally occurring perfect substitution. Customers would be forced to choose dominant incumbents, as they are likely to remain in service, over new entrants and smaller providers. This is seen in the certification industry, which is extremely concentrated [52]. Technically getting website certificate from a smaller certification authority is the same as getting one from a dominant market player. However, there is a longer lifetime for dominant market players, while certificates issued by smaller companies can often be rendered invalid. This reduces the competition in the market and leads to a monopolistic (or oligopolistic market). A discussion of the negative effects of market monopolies is beyond the scope of this paper. However, Asghari et al. [52] note that even when certain certification authorities provide certificates for free, their services are not adopted in the market.

In this case action-based sanctions are likely to be more useful than harm-based sanctions. Ex ante sanctions would ensure that, for example, certification authorities or dynamic DNS providers would meet certain minimum security standards. Lack of compliance would lead to negative consequences through prosecution, which would lead to lower service lifetimes for non-compliant providers. While lack of reliable signaling has lead to a non-functional market for security [53], service lifetimes are a naturally occurring and robust market signal. Thus, prosecution does not need to be perfect, since it would be supported by market's reinforcing phenomena where customers would migrate towards providers with probability of longer service lifetimes.

Alternatively, under harm-based sanctions there may be an over investment in harm mitigation technologies that reduce the probability of harm. However, it is important to note that certain network service providers do not in fact make this

investment. For example, Milton et al. [54] note that Einstein I, which was a voluntary program to secure government networks, saw extremely low rates of adoption. Simultaneously, similar investments in technologies that reduce the magnitude of harm are not made [55]. This may in turn make the injurers insolvent [33].

In general the harm from malware is not evenly distributed across the population, either for network providers or for individuals. For example, it has been noted that a handful of ISPs are responsible for more than 50% of the spam on the network [56]. Similarly, not everyone receives spam. It has been shown that certain email providers are more susceptible to spam that others [57]. Thus, when the probability distribution of harm is varied and known (to the government), action-based sanctions may be more economically efficient than harm based sanctions. Harm-based sanctions may in fact decrease competition in the market and lead to monopolies. Actions-based sanctions would be effective when services are perfectly substitutable, and the cost of sanctions would be subsidized by market forces, given clear signaling.

V. Security vs. Privacy: A Broader Regulatory Discussion

There is an increased effort to regulate the security and privacy landscape online. To the extent that regulation is enabled by sanctions there are two possibilities: action-based sanctions or *ex ante* or harm-based sanctions or *ex post*. There are several limitations to the current approach. First, it is not clear under which scenario action-based sanctions are better vs. harm-based sanctions. Often both are used together, even though they could act as supplements. For example, in the Google Buzz settlement FTC imposed both financial penalties but also audits on future actions [16]. In this paper we compared the economic efficiency, in terms of social welfare, of two exiting policy solutions, one that uses ex ante and a second that employs an ex post regulatory regime.

Overall, when the probability of harm is distributed evenly across the population harm-based sanctions may be preferred. Since harm-based sanction is higher than action-based sanction it leads to more deterrence. Simultaneously, since harm based sanctions are higher, potential injurers should be willing to invest more resources in harm mitigation technologies. Prior research in fact notes over investment especially when investments are non-monetary [33]. Policy should, however, recognize that typically these investments are in technologies that lower the probability of harm and not its magnitude.

TABLE II. Conditions and Results From Less to More Constrained

ex ante	presence of judgement-proof firms
ex post	quotient of the probability of harm and ex-post fine is larger than ex-ante fine
ex-post	governmental perception of harm is higher than actual harm
ex-post	governmental perception of harm is correct low prosecution costs
ex-ante	governmental perception of harm is correct prosecution costs higher than costs of regulatory change
ex-post	governmental perception of harm is correct
ex-ante	governmental perception of harm is lower than actual harm constant probability of harm
ex-ante	government significant user-estimates or over-estimates harm, variable probability of harm

Under harm based sanctions the law is also relatively stable. Fewer individuals are prosecuted under an *ex post* regime. Thus, it is more practical taking into account dual issues of the limited resources of law enforcement and the high cost of prosecution for online breaches [42]. Action based sanctions may be used if market forces (of supply and demand) can subsidize the cost of public enforcement, i.e. when goods or services are perfect substitutes and robust reliable signals for product quality are available to the customer. For example, Camp et al. [58] have suggested an ex ante sanctioning regime, which proposes a cap and trade system for software vulnerabilities to improve software security.

If judgment-proofness is not a concern, harm-based sanctions may be preferred over act-based sanctions, as there are several limitations to action-based sanctions. First, fines for new risks may be underestimated. Second, action-based sanctions would likely be modified as the perceptions of the government change. Changing the law (frequently) is an expensive, tedious, and wasteful exercise. As such action-based sanctions lead to lower deterrence if fines are low. However, high *ex ante* sanctions reduce the amount of the resources the injurer has to invest in risk mitigation technologies. Simultaneously, the injurer would also have fewer resources to address any *ex post* penalties imposed for a breach.

Action-based sanctions are preferred when firms are judgment-proof. For example, 3322.org may not have the resources to provide support to its legitimate users after the takedown operation. Action-based sanctions are also preferred when the harm from an action is not uniformly distributed. Simultaneously, the activity being considered is old and well known, i.e. the government is able to ascertain the probability of harm post hoc. Botnets, for example, are and old and well known. The probability of being a part of the cyber-crime infrastructure is not uniformly spread across all network providers. For example, it has been noted that more than 50% of worldwide spam can be attributed to handful of providers [56], [59]. Under such conditions *ex ante* sanctions are preferable. A possible policy solution can be found in the German anti-botnet initiative. Similar initiatives can provide incentives ISP's to monitor their network for malware infected machines. These incentives do not need to be in terms of mandates. Instead the incentive should be the positive reputation gain for ISPs that provide these services to their customers through public awareness. The success of such a solution would be contingent on the availability of robust market signals, which allow customers to differentiate between ISPs that provide value-added security services and those that don't.

The German anti-botnet initiative considers security to be a public good [9]. An alternative solution is grounded in considering the network as a common-pool resource, being monitored by a group of peers. On a macro level these peers can be ISPs that sanction those who defect by not addressing the vectors of malware on their network [10]. On a micro level peers can form a security club, where individual members improve the security of the network. In this case compromised machines are not sanctioned but cleaned [60]. Garg et al. [11] have similarly proposed peer-based solutions to privacy on OSNs.

In earlier discussions we have considered privacy risks to be independent of security risks. What if we assume that

security and privacy risks are interconnected? For example, a spear phishing email can lead to a data breach that discloses the private keys of thousands of clients. Given that enforcement agencies have a limited amount of resources, should those resources be allocated mitigating security risks or privacy risks?

Lets consider all malware to be one class of software and all technologies that collect private information, for example for behavioral advertising, to be another kind of software. For the software that is malware, we can qualify the software as either impacting the network or the individual on whose system it resides. We combine the malware that impacts user's own system use, for example key loggers, with the privacy infringing software in a general class of spyware [17].

The privacy spyware has two components: the benefit (to the individual) b and the potential harm h. Simultaneously, the spyware that is purely malware has no beneficial component for the individual system owner but only potential harm h. Arguably, then for the same amount of privacy infringing software and malware, social welfare would be higher in the first case than in the second. Thus, the priority for enforcement agencies should be to reduce malware (when both are present in equal amounts).

For example, FTC *ex ante* regulations exclusively focusing on privacy may not be the solution. In fact it may be more appropriate to consider the combined effect of both privacy and security based harms. The goal should be to enforce *ex ante* sanctions on organizations that have failed to invest in due diligence towards security, as security investments have both security and privacy repercussions. Service providers, such as software vendors or network providers generate revenue while exposing the network to (in) security externalities. Thus, the role of the FTC should include engendering *ex ante* sanctions for such firms. For example, it has been argued that Microsoft has quality control concerns during the integration. The lack of within organization enforcement has been attributed to a cultural practice rather than economic costs. As such, the FTC can step in with appropriate *ex ante* sanctions to provide economic incentives that encourage a change in culture. Similar arguments can be made for offending ISPs, dynamic DNS providers, or certification authorities.

VI. Conclusions & Future Work

In this paper we examine a framework that compares two regulatory regimes for sanctions: *ex ante* or action-based sanctions and *ex post* or harm-based sanctions. We investigate its applicability to analyzing sanctions for security and privacy risks online. As the assumptions of the framework are applicable online, the general results are mirror those of Garoupa et al. [23].

Table II does not include all possible market assumptions. **In general, for well known risks where goods and services are perfectly substitutable, and robust market signals are available the economically efficient solution may be ex ante or action based sanctions. For difficult to quantify and/or new risks, where services are not perfect substitutes, (e.g. due to network effects) the better solution may be harm based or ex post sanctions.** Finally, we note that current regulatory and enforcement efforts can lead to less competition in the market and (often) create artificial monopolies.

We applied the general insights to specific cases to to provides insights for online enforcement. Specifically, we examine Do Not Track (a self regulatory privacy effort from market incumbents being supported by the FTC) as well as the FBI's takedown efforts against botnets. DNT is an action-based regime. However, action-based sanctions are more fruitful when risks are familiar, government can estimate the probability of harm, and the distribution of harm over population is known. Privacy is, however, highly contextual [63]. Simultaneously, despite existing laws on data breach disclosure, information on privacy breaches is limited. Given the nature of information technologies, the privacy risks of information collection often new and unknown. Thus, we argue that for privacy sanctioning regime should be harm-based to enable greater social welfare. Given that (new) regulation and lawmaking is expensive and takes time, it is important to have a stable policy regime, which is more likely under ex post sanctions. Ex ante sanctions in this case risks harming market mechanisms for self regulation, by reducing competition, as the cost of entry for new participants is higher than that for incumbents.

FBI's takedown of network providers is a harm-based regime. Harm-based sanctions are admittedly better when risks are new and government systematically underestimates (or overestimates) the probability of harm. However, botnets are a more understood and measurable risk than privacy. Many people want to share information, thus decreasing privacy. It is unlikely that many people want their machines looted for credentials and leveraged for spam. Data on providers whose networks are more infested with bots (or Command and Control servers) is easily available. In fact it has been noted that it is a small set of offenders who are responsible for most of the harm. For example, Eeten et al. note that merely 5 ISP's are responsible for more than 50% of the spam worldwide [64]. Similarly, Garg et al. find that less than 5 countries account for more than 50% spambots [59]. Ex post sanctions in this case reduce competition in the market and create artificial monopolies; since customers would be worried about service lifetimes (and even liability) they would congregate towards established incumbents. Thus, if robust market signals are available to differentiate between two perfectly substitutable goods or services from distinct providers, it is better to have ex ante sanctions. While ex-ante sanctions are expensive, their cost would then be subsidized by market forces of supply and demand. The sanction itself would prevent the creation of artificial monopolies, due to considerations other than security.

The findings in this paper are limited by judgment proof firms. We argue that for privacy harms as enabled by information collection, firms can be prevented from being judgment-proof if they are allowed to sell their databases as assets. This assumes that the market is in perfect competition with several competing organizations, e.g. health care. Alternatively, law enforcement should impose non-monetary sanctions. This would be less of a concern in markets that are oligopolistic. For example, the search engine market only has a handful of participants, e.g. Google, Microsoft. Such participants are currently not judgement-proof. Based on past FTC enforcement efforts the size of fines is typically orders of magnitude lower

than the net worth of the organization.

The finding are of course the limited by ex post and ex ante enforcement in the global economy. However, the entity creating the sanction need not be governmental. For example peering agreements or industry standards such as PCI-DSS could serve as sanctions.

This work is also limited by the assumptions of the model. We assumed that the probability of detection *ex ante* and *ex post* would be the same. In practice these probabilities would be different. Offline, it could be less expensive to observe if there is an oil spill than to ensure that all oil containers match a specific standard. Does this transfer online? Similarly, we also assume that the cost of conviction is the same *ex ante* and *ex post*. This may be true for familiar, well known risks. However, for new risks the costs may be higher *ex ante* than *ex post*.

Finally, the extended model assumed that the probability of harm is not uniformly distributed over the entire population. However, this may also be true for the magnitude of harm. Lets consider the case of anonymized data disclosure. There is a higher privacy violation for individuals with more unique characteristics as more information can be gleaned about them. As such under-represented groups, which tend to be more vulnerable populations, will suffer more. For example, it may be embarrassing for a heterosexual person to have their sexual history disclosed. For a queer person this may significant consequences that go beyond embarrassment (e.g. financial and social discrimination.)

ACKNOWLEDGEMENTS

The research was sponsored by ARL Cyber Security CRA W911NF-13-2-0045, DHS Contract N66001-12-C-0137, and Google. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the DHS, ARL, DoD, Google, IU or any official policies of any of these entities.

REFERENCES

[1] R. Böhme and S. Koble, "On the viability of privacy-enhancing technologies in a self-regulated business-to-consumer market: Will privacy remain a luxury good," in *Workshop on Economics of Information Security*, 2007.

[2] R. Rowlingson and R. Winsborrow, "A comparison of the payment card industry data security standard with ISO17799," *Computer Fraud & Security*, vol. 2006, no. 3, pp. 16–19, 2006.

[3] Ponemon, "Economic impact of privacy on online behavioral advertising," Ponemon Institute, Tech. Rep., 2010.

[4] S. Preibusch and J. Bonneau, "The privacy landscape: Product differentiation on data collection," *Economics of Information Security and Privacy III*, pp. 263–283, 2011.

[5] C. Soghoian, "How dropbox sacrifices user privacy for cost savings," Slight Paranoia Blog, Tech. Rep., 2011.

[6] R. Anderson and T. Moore, "The economics of information security," *Science*, vol. 314, no. 5799, pp. 610–613, 2006.

[7] H. Varian, "System reliability and free riding," *Economics of Information Security*, pp. 1–15, 2004.

[8] H. Garett, "The tragedy of the commons," *Science*, vol. 162, pp. 1243–1248, 1968.

[9] D. K. Mulligan and F. B. Schneider, "Doctrine for cybersecurity," *Daedalus*, vol. 140, no. 4, pp. 70–92, 2011.

[10] L. J. Camp, "Reconceptualizing the role of security user," *Daedalus*, vol. 140, no. 4, pp. 93–107, 2011.

[11] V. Garg, S. Patil, A. Kapadia, and L. J. Camp, "Peer-produced privacy protection," in *Proceedings of IEEE Symposium on Technology and Society*, 2013.

[12] S. Shavell, "Liability for harm versus regulation of safety," *The Journal of Legal Studies*, vol. 13, no. 2, pp. 357–374, 1984.

[13] S. Romanosky and A. Acquisti, "Privacy costs and personal data protection: Economic and legal perspectives," *Berkeley Tech. LJ*, vol. 24, p. 1061, 2009.

[14] B. A. Huberman, E. Adar, and L. R. Fine, "Valuating privacy," *Security & Privacy, IEEE*, vol. 3, no. 5, pp. 22–25, 2005.

[15] FTC, "A preliminary ftc staff report on protecting consumer privacy in an era of rapid change: A proposed framework for businesses and policymakers," Federal Trade Commision, Tech. Rep., 2010.

[16] E. Newland, "Ftc-google "buzz" settlement sets new norm for privacy," Center for Democracy & Technology, Tech. Rep., 2011.

[17] H. Ng Osborn, "Targeting bad behavior: Why federal regulators must treat online behavioral marketing as spyware," *Hastings Communication & Entertainment Law Journal*, vol. 31, p. 369, 2008.

[18] D. Hirsch, "The law and policy of online privacy: Regulation, self-regulation, or co-regulation?" *Seattle University Law Review*, vol. 34, no. 2, 2011.

[19] A. Goldfarb and C. E. Tucker, "Privacy regulation and online advertising," *Management Science*, vol. 57, no. 1, pp. 57–71, 2011.

[20] E. Goldman, "A coasean analysis of marketing," *Wisconsin Law Review*, pp. 1151–1221, 2006.

[21] S. Ramasubramanian, "Microsoft's takedown of 3322.org - a gigantic self goal?" CircleID, September 17, 2012. Available: http://www.circleid.com/posts/20120917_microsoft_takedown_of_3322_org_a_gigantic_self_goal/ [Last Accessed: June 15, 2013], 2012.

[22] B. Schneier, "The fbi's wiretapping plan is great news for criminals," Foreign Policy, May 29, 2013. Available: http://www.foreignpolicy.com/articles/2013/05/29/the_fbi_s_new_wiretapping_plan_is_great_news_for_criminals/ [Last Accessed: June 15, 2013], 2012.

[23] N. Garoupa and M. Obidzinski, "The scope of punishment: An economic theory," *European Journal of Law and Economics*, vol. 31, no. 3, pp. 237–247, 2011.

[24] T. Bandyopadhyay, V. S. Mookerjee, and R. C. Rao, "Why IT managers don't go for cyber-insurance products," *Communications of the ACM*, vol. 52, no. 11, pp. 68–73, 2009.

[25] W. Seltzer, "Free speech unmoored in copyright's safe harbor: Chilling effects of the DMCA on the first amendment," *Harvard Journal of Law & Technology*, vol. 24, no. 1, pp. 171–232, 2010.

[26] J. Yan, N. Liu, G. Wang, W. Zhang, Y. Jiang, and Z. Chen, "How much can behavioral targeting help online advertising?" in *Proceedings of the 18th international conference on World wide web*. ACM, 2009, pp. 261–270.

[27] D. S. Evans, "The online advertising industry: Economics, evolution, and privacy," *Journal of Economic Perspectives*, vol. 23, no. 3, pp. 37–60, 2009.

[28] A. M. Polinsky and S. Shavell, "The economic theory of public enforcement of law," *Journal of Economic Literature*, vol. 38, no. 1, pp. 45–76, 2000.

[29] V. Garg, "Intellectual freedom in India," 2012.

[30] P. P. Gunn, A. M. Fremont, M. Bottrell, L. R. Shugarman, J. Galegher, and T. Bikson, "The health insurance portability and accountability act privacy rule: a practical guide for researchers," *Medical care*, vol. 42, no. 4, pp. 321–327, 2004.

[31] M. Rosenberg, "Analysis: Bp's u.s. gulf oil spill settlement challenges may backfire," Reuters, Tech. Rep., 2014.

[32] G. S. Becker, "Crime and punishment: An economic approach," *The Journal of Political Economy*, vol. 76, no. 2, pp. 169–217, 1968.

[33] G. Dari-Mattiacci and G. De Geest, "When will judgment proof injurers take too much precaution?" *International Review of Law and Economics*, vol. 26, no. 3, pp. 336–354, 2006.

[34] R. Pitchford, "How liable should a lender be? the case of judgment-proof firms and environmental risk," *The American Economic Review*, pp. 1171–1186, 1995.

[35] K. Stech, "Burglary triggers medical records firm's collapse," The Wall Street Journal, March 12, 2012. Available: http://blogs.wsj.com/bankruptcy/2012/03/12/burglary-triggers-medical-records-firm's-collapse/ [Last Accessed: June 15, 2013], 2012.

[36] S. Shavell, "The judgment proof problem," *International Review of Law and Economics*, vol. 6, pp. 45–58, 1986.

[37] D. van Zyl Smit, "Life imprisonment: recent issues in national and international law," *International Journal of Law and Psychiatry*, vol. 29, no. 5, pp. 405–421, 2006.

[38] D. Bronski, C. Chen, M. Rosenthal, and R. Pluscec, "FTC vs. Toysmart," *Duke Law & Technology Review*, vol. 1, no. 1, p. 12, 2001.

[39] O. Hathaway, "Path dependence in the law: The course and pattern of legal change in a common law system," *The Iowa Law Review*, vol. 86, no. 2, pp. 101–165, 2001.

[40] R. Böhme and G. Schwartz, "Modeling cyber-insurance: Towards a unifying framework," in *Workshop on Economics of Information Security*, 2010.

[41] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in *Proceedings of the Workshop on the Economics of Information Security*. Springer, 2012.

[42] D. S. Wall, "Policing cybercrimes: Situating the public police in networks of security within cyberspace," *Police Practice and Research*, vol. 8, no. 2, pp. 183–205, 2007.

[43] S. Musil, "Developer defends girls around me app," CNET, Tech. Rep., 2012.

[44] P. Eckersley, "How unique is your web browser?" in *Privacy Enhancing Technologies*. Springer, 2010, pp. 1–18.

[45] R. A. Posner, "The economics of privacy," *The American economic review*, vol. 71, no. 2, pp. 405–409, 1981.

[46] D. Sullivan, "Duck duck go's post-prism growth actually proves no one cares about "private" search," Search Engine Land, Tech. Rep., 2013.

[47] D. J. Solove, "I've got nothing to hide and other misunderstandings of privacy," *San Diego Law Review*, vol. 44, p. 745, 2007.

[48] K. Hill, "How target figured out a teen girl was pregnant before her father did," Forbes, Tech. Rep., 2012.

[49] T. B. Lee, "Here's everything we know about prism to date," Washington Post, Tech. Rep., 2013.

[50] M. L. Katz and C. Shapiro, "Systems competition and network effects," *The Journal of Economic Perspectives*, vol. 8, no. 2, pp. 93–115, 1994.

[51] A. Acquisti, A. Friedman, and R. Telang, "Is there a cost to privacy breaches? an event study," in *Fifth Workshop on the Economics of Information Security*, 2006.

[52] H. Asghari, M. Van Eeten, A. Arnbak, and N. Van Eijk, "Security economics in the https value chain," in *Workshop on the Economics of Information Security*, 2013.

[53] B. Edelman, "Adverse selection in online trust certifications," in *Fifth workshop on the economics of information security*, 2006, pp. 26–28.

[54] M. Mueller and A. Kuhn, "Einstein on the breach: Surveillance technology, cybersecurity and organizational change," in *Workshop on the Economics of Information Security*, 2013.

[55] T. R. Beard, "Bankruptcy and care choice," *The RAND Journal of Economics*, pp. 626–634, 1990.

[56] M. Van Eeten, J. Bauer, J. Groenewegen, and W. Lemstra, "The economics of malware," in *Telecommunications Policy Research Cconference*, 2007.

[57] I.-H. Hann, K.-L. Hui, Y.-L. Lai, S. Y. T. Lee, and I. Png, "Who gets spammed?" *Communications of the ACM*, vol. 49, no. 10, pp. 83–87, 2006.

[58] L. J. Camp and C. Wolfram, "Pricing security," in *Proceedings of the CERT Information Survivability Workshop*, 2000, pp. 31–39.

[59] V. Garg, T. Koster, and L. J. Camp, "Cross-country analysis of spambots," Indiana University, Tech. Rep., 2012.

[60] Z. Dong, V. Garg, L. J. Camp, and A. Kapadia, "Pools, clubs and security: designing for a party not a person," in *Proceedings of the 2012 workshop on New security paradigms*, ser. NSPW '12. New York, NY, USA: ACM, 2012, pp. 77–86.

[61] J. P. Caulkins, D. Grass, G. Feichtinger, and G. Tragler, "Optimizing counter-terror operations: Should one fight fire with "fire" or "water"?" *Computers & Operations Research*, vol. 35, no. 6, pp. 1874–1885, 2008.

[62] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage, "Spamalytics: an empirical analysis of spam marketing conversion," *Communications of the ACM*, vol. 52, no. 9, pp. 99–107, 2009.

[63] H. F. Nissenbaum, *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law & Politics, 2010.

[64] M. van Eeten, J. M. Bauer, H. Asghari, and S. Tabatabaie, "The role of internet service providers in botnet mitigation: An empirical analysis based on spam data," OECD Publishing, OECD Science, Technology and Industry Working Papers 2010/5, May 2010. [Online]. Available: http://dx.doi.org/10.1787/5km4k7m9n3vj-en