Supplementary material

Proofs

As mentioned in the paper we remind the reader that all proofs in this supplementary material prove the lemmas and theorems for positive consensuses. However, proving these lemmas and theorems for negative ones is straightforward, changing No^+, No^{+*}, Con^+ *app*, and *app** for No^-, No^{-*}, Con^- *inapp*, and *inapp**.

Lemma 1. *Con^+ is the smallest search space for positive consensuses.*

Before addressing the proof of the lemma we introduce and prove an auxiliary lemma

Lemma 2. *Let $c \in C$ be a context such that $c_1, \ldots, c_k \in C$ are such that c_1 g c, $\ldots$, c_k g c, then $(c_1 \wedge \cdots \wedge c_k)$ g c*

Proof (Lemma 2)**.** *Suppose $c, c_1, \ldots, c_n \in C$, such that c_1 g c, $\ldots$, c_n g c, then $c_1 \wedge \cdots \wedge c_n$ g c, because if c is true then all $c_1, \ldots, c_n$ are true as they generalise c, thus $c_1 \wedge \cdots \wedge c_n$ is also true. However, if $c_1 \wedge \cdots \wedge c_n$ is true c does not necessarily have to be true. For example, in the case of sharing data these context could represent possible recipients like $c_1 = family$, $c_2 = living\_in\_home$, $c = son$. Then, there might be recipients who satisfy $family \wedge living\_in\_home$ yet do not satisfy son. Thus, $c_1 \wedge \cdots \wedge c_n$ is more general than c.*

Proof (Lemma 1)**.** *We have to prove that all positive consensuses are in Con^+, and that any subset of Con^+ cannot be a valid search space for positive consensuses. We first show that all positive consensuses are in Con^+.*

Let $a \in A$ be an action and $c \in C$ be a context formula over which there is a positive consensus ($app^*(c) = U$). Let $c_1, \ldots, c_k \in C$ be contexts such that $c = c_1 \wedge \cdots \wedge c_k$, where $c_1, \ldots, c_k$ are context formulas with no $\wedge$ operators. Without loss of generality we can assume $c_1, \ldots, c_r \notin Con^+$ ($r \leq k$) and $c_r, \ldots, c_k \in Con^+$. Note that $c_1, \ldots, c_r \in No^{+*} \setminus Con^+$ because the contexts $c \in No \setminus No^{+*}$ either have $inapp(c) \neq \emptyset$ (which cannot be part of a positive consensus) or $app^*(c) = \emptyset$ (which would make the consensus redundant and less general). Let $con \in \{c_1, \ldots, c_r\}$ be a context in the positive consensus, such that $con \in No^{+*} \setminus Con^+$, from the definition of Con^+, we know that then $\exists con_1, \ldots con_s \in Con^+$, such that con_1 g con, $\ldots$, con_s g con, furthermore from the definition of the preference propagation, since $con \notin No^+$, we

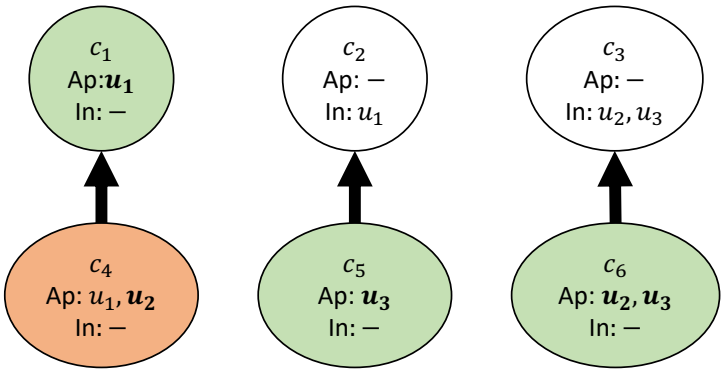

Figure 1: Preference graph (with propagated preferences), each node represents one of the contexts $(c_1, \ldots, c_6)$, and has an associated list of users that find the context appropriate (Ap) and inappropriate (In). The original preferences are highlighted in bold font, whereas propagated approval preferences are in normal font. The coloured nodes are the ones in $Con^+ = No^{+*} \setminus Exc$, note the node in orange is in Con^+ because it cannot be excluded as it is part of No^+. Therefore the coloured nodes are those in Con^+, whereas those uncoloured are in No^- in this case.

know $app(con) = \emptyset$ *and* $\forall u \in app^*(con)$, $\exists con_u \in \{con_1, \ldots, con_s\}$ *such that* con_u *g* con *and* $u \in app(con_u)$. *Then if* $app^*(con) = \{u_1, \ldots, u_r\}$ *we have that* $con_{u_1} \wedge \cdots \wedge con_{u_r}$ *(were these might not all be different contexts) is formed of contexts in* Con^+, *with* $app^*(con) \subseteq app^*(con_{u_1}) \cup \cdots \cup app^*(con_{u_r})$ *and as shown in the previous Lemma 2,* $(con_{u_1} \wedge \cdots \wedge con_{u_r})$ *g* con. *Hence, the context* c' *which is like* c *replacing each* $con \in \{c_1, \ldots, c_r\}$ *for their corresponding* $con_{u_1} \wedge \cdots \wedge con_{u_r}$, *is more general than* c. *Furthermore,* c' *is formed of contexts in* Con^+, *and* $app^*(c') = U$, *hence we have found a positive consensus made from contexts in* Con^+ *which generalises the one we have supposed is not made from contexts in* Con^+, *thus proving* Con^+ *is a search space for the norm consensus problem.*

Now we show that any subset of Con^+ *is not a complete search space, we prove this with a counterexample. Suppose three users* $U = \{u_1, u_2, u_3\}$, *an action* a *and six contexts* $C = \{c_1, \ldots, c_6\}$ *with (propagated) preference graph as in Figure 1. In this case, the positive consensuses we aim at detecting are* $\{c_1, c_6\}$, *and* $\{c_4, c_5\}$ *because all other combinations of contexts that are jointly approved by all users are generalised by one of these two (e.g.* $\{c_4, c_6\}$ *is also approved by all users but* $\{c_1, c_6\}$ *generalises it), or contain more contexts than needed making them less general (e.g.* $\{c_1, c_5, c_6\}$ *where* c_5 *is redundant). In this case, the coloured contexts are the ones in* Con^+, *if we remove any of these nodes from the search space then we would not find all of the aforementioned consensuses. Therefore, in general terms,* Con^+ *is the smallest search space possible.*

Theorem 1. *N is the solution of the norm consensus problem.*

To prove Theorem 1, we divide it into two sub-theorems, if we prove these two sub-theorems, then Theorem 1 follows.

Theorem 2. *N satisfies the preference representation, and maximally regulatory properties.*

Theorem 3. *N satisfies the minimality property.*

Proof (Theorem 2)**.** *First of all, the preference alignment property is satisfied by the way the norms are constructed. This property requires that all permission/prohibition norms have a positive/negative consensus over their pair of action and context precondition. Our methodology to obtain the norms actually detects consensuses first and then constructs the norms from them, thus this property is naturally satisfied.*

When it comes to maximally regulatory norms, suppose through the approach presented in Section 4 we obtain a set of norms N but there is a set of norms N_{max} which is preference aligned and maximally regulatory. Note that since we use logical formulas to define the preconditions of norms, for N_{max} to be maximally regulatory and N not to, there must be a context $c \in C$ such that c activates one norm $n \in N_{max}$ while it does not activate any norms of N. Let (φ, a) be the precondition and action of n, since N_{max} is preference aligned, then it follows that there is a positive/negative consensus over (φ, a). Without loss of generality we can assume this is a positive consensus (a similar argument can be made for negative ones), then we have that $\varphi = c \wedge c_1 \wedge \cdots \wedge c_k$ and $\cup_{con \in \{c,c_1,\ldots,c_k\}} app^*(con) = U$ and $\cup_{con \in \{c,c_1,\ldots,c_k\}} inapp(con) = \emptyset$. Since the approach in Sec. 4.2 finds all consensus until there are no solutions left for the BIP, $\{c, c_1, \ldots, c_k\}$ is not a solution of the BIP presented in Sec. 4.2. This can only happen when these contexts are ineligible due to some constraint. We know $\{c, c_1, \ldots, c_k\}$ satisfies the coverage constraint as the approval users for the contexts fully cover U, so the constraint that is not satisfied must be a generalisation or a found consensus constraint. On the one hand, suppose $\{c, c_1, \ldots, c_k\}$ is ineligible because of a generalisation constraint, this means there is at least one pair $(c_i, c_j) \in \{c, c_1, \ldots, c_k\}^2$ such that c_i g c_j, but this means $\{c, c_1, \ldots, c_k\}$ is redundant and there is a smaller set of contexts $S \subseteq \{c, c_1, \ldots, c_k\}$ which is part of one of our consensus, meaning our set satisfies maximal regulation as it would have a norm whose precondition is more general than that of φ. Lastly, $\{c, c_1, \ldots, c_k\}$ might be ineligible because of a found consensus constraint, but this means that there is a consensus $con = \{c'_1, \ldots, c'_s\}$ such that, each of the contexts in con either is also in or generalises a context in $\{c, c_1, \ldots, c_k\}$. Which again means that the resulting precondition from con $\varphi_{con} = c'_1 \wedge \cdots \wedge c'_s$ is more general than φ, thus contradicting the assumption that N_{max} is maximally regulatory.

Proof (Theorem 3)**.** *Let $a \in A$ be an action such that N, the set of norms obtained with our approach, is not minimal and instead there is a set of norms N_{min} which is maximally regulatory like N but is it's minimal $|N_{min}| < |N|$.*

Let $\varphi_1, \ldots, \varphi_k$ be the preconditions of the norms in N, or in other words, all the consensuses found using our approach, and let $\varphi'_1, \ldots, \varphi'_s$ be the preconditions of the minimal set of norms N_{min}. Note that as we have demonstrated above, $\varphi_1, \ldots, \varphi_k$ and $\varphi'_1, \ldots, \varphi'_s$ are in either Con^+ or Con^-, furthermore in this case we suppose $s < k$. Suppose C_{reg} is the set of all regulated contexts (that is, a $c \in C_{reg}$ will always activate at least one norm of both N and N_{min}). We prove the theorem distinguishing two cases.

First, let $c \in C_{reg}$ be a regulated context such that if φ_i is the precondition of a norm in N regulating it, then there is no more specific logic formula formed from contexts in Con^+ or Con^- that is activated by c. In this case we have that if φ'_j is the precondition of a norm in N_{min} regulating context c, then we have that either $\varphi'_j = \varphi_i$ or $\varphi'_j \ g \ \varphi_i$. Note though that it must be $\varphi'_j = \varphi_i$ because if $\varphi'_j \ g \ \varphi_i$, then the target function of our BIP would have a lower value for the set of contexts of φ'_j than for those of φ_i. Since our BIP approach found the consensus context φ_i and not φ'_j despite minimising the target function, it means that φ'_j must break some of the constraints. φ'_j satisfies the generalisation and found consensus constraints because if it did not then φ_i would not either (and we know it does). Therefore, the only possibility is that φ'_j is not consensual (it does not satisfy the coverage constraint). Hence, since we know φ'_j is consensual, it must then be $\varphi'_j = \varphi_i$.

Second, without loss of generality, we assume that all $\varphi_1, \ldots, \varphi_k$ and $\varphi'_1, \ldots, \varphi'_s$ are different (we focus only on those preconditions that are different, since we are "removing" those that are equal in both sets and both sets satisfy maximal regulation, the remaining preconditions will describe exactly the same contexts). Let $c \in C_{reg}$ be a regulated context that activates φ_i having discarded the case above, we now suppose we can build at least one more specific logic formula in Con^+ or Con^- that is activated in context c. In this case, the context φ'_j could either be one of this more specific context logic formulas or be equal to φ_i. Since our logic only considers the contexts in C and the operator $\wedge$, if φ'_j is a more specific formula than φ_i ($\varphi_i \ g \ \varphi'_j$) it means that the contexts that are in φ_i and not in φ'_j have to be regulated by another $\varphi'_q \in \{\varphi'_1, \ldots, \varphi'_s\}$ because both sets are maximally regulatory. If φ'_q is $\varphi'_q = \varphi_i$ then the norm with precondition φ'_j is redundant meaning N_{min} is not minimal. If $\varphi'_q \ g \ \varphi_i$, then applying a similar reasoning to that on the first case, we have that φ'_q is not consensual. Finally, if $\varphi_i \ g \ \varphi'_q$, then again N_{min} is not minimal because we can remove both norms with preconditions φ'_j and φ'_q and add the norm with preconditionφ_i to get a maximally regulatory set of norms with less norms than N_{min}.

Therefore $|N_{min}| < |N|$ is not possible, meaning that our N is minimal.